Discrete Time Quantum Lattice Systems

Von der Fakultät für Elektrotechnik, Informationstechnik, Physik
der Technischen Universität Carolo-Wilhelmina
zu Braunschweig
zur Erlangung des Grades eines
Doktors der Naturwissenschaften
(Dr.rer.nat)
genehmigte
D i s s e r t a t i o n

von Holger Vogts
aus Westerstede

1. Referent: Prof. Dr. Reinhard F. Werner
2. Referent: PD Dr. Michael Keyl
eingereicht am: 12.03.2009
mündliche Prüfung (Disputation) am: 25.06.2009
Druckjahr: 2009

Vorveröffentlichungen der Dissertation

Teilergebnisse aus dieser Arbeit wurden mit Genehmigung der Fakultät für Elektrotechnik, Informationstechnik, Physik, vertreten durch den Mentor der Arbeit, in folgenden Beiträgen vorab veröffentlicht:

Publikationen

> Dirk M. Schlingemann, Holger Vogts & Reinhard F. Werner: *On the structure of Clifford quantum cellular automata.* J. Math. Phys. 49:112104 (2008)

Tagungsbeiträge

1. Holger Vogts & Reinhard F. Werner: *On the connection between quantum walks and quantum cellular automata.* (Vortrag) DPG – Frühjahrstagung, Frankfurt, März 2006
2. A. Gattner, H. Vogts, T. Franz & R. F. Werner: *Reversible Quantum Cellular Automata.* (Poster) Workshop on "Cats, Kets and Cloisters", Oxford, Juli 2006
3. Holger Vogts & Reinhard F. Werner: *Invariance of quantum cellular automata under all lattice symmetries.* (Vortrag) DPG – Frühjahrstagung, Düsseldorf, März 2007
4. Holger Vogts & Reinhard F. Werner: *Invariance of quantum cellular automata under all lattice symmetries.* (Poster) Workshop on "Quantum Information and Many-Body Quantum Systems", Pisa, März 2007
5. Holger Vogts & Reinhard F. Werner: *Particle number conserving quantum cellular automata and quantum walks.* (Poster) Workshop on "Quantum Engineering with Neutral Atoms and Light", Herrsching, Juni 2007
6. Holger Vogts, Dirk M. Schlingemann & Reinhard F. Werner: *Clifford quantum cellular automata and translationally invariant stabilizer states.* (Vortrag) 5th Central European Quantum Information Processing Workshop (CEQIP), Telč, Juni 2008
7. Holger Vogts & Reinhard F. Werner: *Index theory of quantum walks and quantum cellular automata.* (Vortrag) A2-Meeting, Potsdam, Dezember 2008

Abstract

Discrete time quantum lattice systems recently have come into the focus of quantum computation because they provide a versatile tool for many different applications and they are potentially implementable in current experimental realizations. In this thesis we study the fundamental structures of such quantum lattice systems as well as consequences of experimental imperfections.

Essentially, there are two models of discrete time quantum lattice systems, namely quantum cellular automata and quantum walks, which are quantum versions of their classical counterparts, i.e., cellular automata and random walks. In both cases, the dynamics acts locally on the lattice and is usually also translationally invariant. The main difference between these structures is that quantum cellular automata can describe the dynamics of many interacting particles, whereas quantum walks describe the evolution of a single particle.

The first part of this thesis is devoted to quantum cellular automata. In Chapter 3 we establish an index theory for one-dimensional quantum cellular automata. This index is a locally computable quantity, which is constant along the line, even without assuming translation invariance. In Chapter 4 we characterize in detail a subclass of quantum cellular automata by requiring that Pauli operators are mapped to Pauli operators. These evolutions are called Clifford quantum cellular automata, and their structure can be understood in terms of certain classical cellular automata. In Chapter 5 we study systems for which all lattice symmetries are conserved and not only translations.

The second part of this thesis is concerned with quantum walks. We show in Chapter 6 that every quantum walk can be identified with the one-particle sector of a quantum cellular automaton, i.e., with the one-particle restriction of an interacting many particle system. We also find different factorizations for quantum walks, leading to different construction techniques for quantum cellular automata out of a given quantum walk. In Chapter 7 we establish an index theory for quantum walks with analogous results to the case of cellular automata. Finally, we discuss decoherent quantum walks in Chapter 8, i.e., the behavior of quantum walks with experimental imperfections.

Contents

Chapter 1

Introduction

This Chapter is devoted to illustrating the subject of this thesis in the larger context of quantum computation, which is one of the main applications of quantum information theory. Of course, this presentation is far from being comprehensive and gives only a brief overview of the field. More elaborate introductions can, for instance, be found in [NC00, Key02, ABH$^+$01, Pre99].

1.1 Quantum Computation

Quantum information is a rather new and interdisciplinary field of research, as there are physicists, both experimental and theoretical, mathematicians and computer scientists concerned with this topic. The basic idea is to use quantum systems as the carriers of information, i.e., the information is encoded in the quantum state of the system. Hence, concepts of quantum theory, like superposition and entanglement, become meaningful for information processing, leading to many new applications and phenomena. In quantum information the states are usually described in abstract terms and independent of the physical realization. Corresponding to the classical bit, the smallest quantum information unit is a *qubit*, which describes any two-level quantum system.

One of the most striking applications of quantum information is *quantum computation*. The long term goal of quantum computation is to build devices, which are based on quantum operations, and which outperform any existing or future classical computer. The possibility of doing this was first presented by Shor in his famous factorization algorithm paper [Sho94, Sho97], in which he constructed a quantum algorithm to decompose any integer into its prime factors. In contrast to all known classical algorithms, which require exponential time in the number of digits, Shor's algorithm runs in polynomial time.

Many schemes, which are capable of universal quantum computation, have been invented, i.e. these structures are able to efficiently simulate any quantum computation. Most of these schemes are quantum versions of classical mod-

els, e.g. *quantum circuit model*, *quantum Turing machine* [Deu85] or *quantum cellular automata* [Wat95]. However, the structure of quantum mechanics also allows for computation schemes, which do not have a classical analogue, e.g. by using entangled states as resource for the computation. The most prominent of these examples is the *one-way quantum computer* introduced by Briegel and Raussendorf [RB01, RB02]. In this scheme the quantum computation is replaced by a sequence of measurements on a highly entangled state on a two dimensional lattice of qubits. This special state is called *cluster state*, and it can be generated out of a product state by a single time step of a quantum cellular automaton. Recently, also other resource states for measurement based computation have been discussed [GE07, GESPG07].

However, a universal quantum computer is far from being experimentally realized. In the near future it seems more promising to build special devices, which are able to simulate complex quantum systems. This concept of *quantum simulation* goes back to the groundbreaking work of Feynman [Fey82]. He noticed the rapid growth of complexity in solid state models as the lattice size is increased, and therefore suggested to use controllable quantum systems for the simulation of these models. Indeed, the Hilbert space dimension, and thereby the number of parameters needed for a description of general states, grows exponentially with the number of particles. Nevertheless, there are also many efforts to find an efficient classical description of many-body systems, in some cases even with the help of techniques from quantum information science. Recently, one of the most common concepts has been a parametrization of many-body states in terms of matrix product states [ÖR95] or projected entangled pair states [VC04, VWPGC06] (in higher lattice dimensions), which are based on the notion of finitely correlated states [FNW92]. For instance, these states are well-suited to describe ground states of gapped local Hamiltonians [Has07], but a simulation of the time evolution with such techniques fails [SWVC08]. Therefore, time evolution of local Hamiltonians seems to be a promising task for quantum simulators.

There are many attempts to experimentally realize devices, which are capable of doing useful quantum computational tasks. However, up to now no realization satisfies all the requirements for universal comuputation, e.g. given by the DiVincenco criteria [DiV00]. For example, the control of the desired operations is often not perfectly accurate, which ultimately destroys coherent superpositions. The first proposals for an experimental implementation of quantum computation are based on NMR systems [Llo93, DiV95] and trapped ions [CZ95]. Indeed, with both techniques many steps towards quantum computation have been experimentally realized (for instance, see [VSB$^+$01] for NMR and [SKHR$^+$03] for ion traps), but scalability seems to be a problem in these systems. More recently, systems of neutral atoms in optical lattices [JBC$^+$99] or in arrays of magnetic micro traps [BF06] have been considered. One of the most amazing demonstrations of the power of neutral atoms in optical lattices, especially for quantum simulation, is the transition between Mott-insulating phase and superfluid phase [GME$^+$02].

However, single sites cannot be easily addressed in these realizations, which limits their use as quantum computers. In contrast, global transformations are relatively easy to implement, which together with the underlying lattice structure gives one of the main motivations for the study of quantum cellular automata.

1.2 Quantum Cellular Automata & Quantum Walks

Quantum cellular automata and quantum walks are analogues of the corresponding classical concepts, namely *cellular automata* and *random walks*. In both cases the underlying structure are lattices. In a cellular automaton each lattice point labels a *cell* (or *site*), which is associated with a finite alphabet, e.g. in the simplest case with a bit $\{0, 1\}$. The cellular automaton describes a transformation of the values of the cells, i.e. a discrete time step, which is also called the *global rule*. In the process, the value of a single cell at time $t + 1$ should only depend on the values of finitely many cells at time t. The positions of these cells form the *neighborhood scheme* of the cellular automaton. The global time step can therefore be described by applying a *local rule* in parallel to all cells.

Many examples of cellular automaton rules have been intensively studied, the most famous one of which is Conway's "Game of Life" [BCG82]. The rather simple description in terms of local rules and the ability of producing complex behavior are the most striking features of cellular automata. Therefore, in many fields of research they have become a powerful tool, and many special cellular automaton rules have been highly developed for several applications, such as coffee percolation or highway traffic, e.g. the Nagel-Schreckenberg model [NS92]. Furthermore, cellular automaton rules naturally arise by discretizing partial differential equations, e.g., by introducing finite time steps and discrete space coordinates in a diffusion equation.

Since cellular automata provide a versatile and powerful tool in computer science and its applications, there have been several attempts to introduce a quantized version of them. Intuitively, the idea of *quantum cellular automata* (QCAs for short) is quite clear. One just has to replace the finite alphabet in each cell by a finite dimensional quantum system and the cellular automaton rule by a local, translationally invariant quantum transformation. A first attempt of doing this is already present in Feynman's idea of quantum simulation [Fey82]. However, he did not come up with a detailed description of what a quantum cellular automaton should be, and in the early years quantum computation was mainly based on the circuit model. A QCA like quantum computation scheme was at first proposed by Lloyd [Llo93] (see also [Ben00]) for NMR systems. His scheme circumvents the addressing constraints on a chain of alternating atom types by applying the same gate operations to all atoms of the same type, and

he showed that, nevertheless, useful quantum computation is possible to some extent.

However, a formal definition of QCAs was missing for a long time. One of the first serious attempts of doing this was given by Watrous [Wat95]. Unfortunately, his definition has serious flaws, as the connection between global rule and local rule is not quite clear. It is not easy to decide whether a given Watrous automaton is reversible ("well-formed" in this language), and the study of quantum cellular automata was for a few years mainly concerned with finding efficient decision procedures for this question [DS96, DTS97] (see also [Arr06]). Furthermore, a product of two Watrous automata may fail to be a valid Watrous automaton. Because of all these inconsistencies, the study of QCAs did for a long time not get that far as one would have expected.

Certainly, one has to admit that there are serious problems when one wants to pass from classical to quantum cellular automata, starting with a rigorous definition of the quantum system itself, as there are infinitely many cells around. Also finding a suitable notion of locality seemed to be a problem. Using techniques from statistical mechanics of quantum spin systems, namely by looking at the observable algebra rather than states, these problems can be circumvented. Such techniques have been used first in [RW95], but only for special cellular automaton rules and not for an axiomatic definition. An operator algebraic approach was also used in [Pas02], however for the states and not for the observables of the system, somehow mixing up Schrödinger and Heisenberg evolution.

The first satisfactory definition of QCAs was given by Schumacher and Werner, although only for the class of reversible ones [SW04]. In their definition the connection between global and local rule is precisely clear and the locality is formulated as follows: The state at time t restricted to some finite region should only depend on the state at time $t-1$ restricted to some slightly larger region, i.e., no signals can be send from far apart constituents in one time step.

Nevertheless, there are still attempts to establish alternative definitions of QCAs. In [PDC05, PDC07] a QCA is up to a one-site operation defined by a single local unitary operator, which is supposed to commute with all its translates. This corresponds to the simplest of the basic construction schemes in [SW04], and is indeed sufficient for many useful applications. However, this definition excludes simple shift operations. But running a right shift on one system and a left shift on an additional system gives in total a QCA satisfying the definition, i.e. a QCA is decomposed into individual dynamical systems, which are not considered as QCAs. Since shifts are also easily implemented in many experiments, we prefer the definition of [SW04]. An overview on all quantum cellular automata models can be found in [Wie08].

Similar to the classical cellular automaton model of Margolus [Mar84] a constructive approach of QCAs is to use partitioned ones. Here the lattice is divided into blocks of cells and the same unitary transformation is applied to each single block. Using different block structures and block unitaries one obtains a versatile

construction method. These *partitioned quantum cellular automata* are common to most models of general QCAs. Hence, studies based on such constructions, e.g. [BW03], are independent of the formal definition. Now an interesting question is whether all QCAs, which satisfy the axiomatic definition, can be obtained by such a partitioning scheme (or *local implementation scheme*). Recently, Arrighi, Nesme and Werner have shown that this is indeed possible, if one allows for an additional ancilla system at each lattice site [ANW08].

Similar to the classical case there are several applications of quantum cellular automata. First of all, they provide an abstract quantum computation model. For instance, QCAs are computationally equivalent to the quantum circuit model and the quantum Turing machine [Wat95, vD96], i.e., all these models are able to efficiently simulate each other. More recently, several schemes for universal quantum computation in QCA structures have been discussed, e.g. Raussendorf's QCA on a two dimensional lattice [Rau05a]. Also in one lattice dimension quantum cellular automata, which are capable of universal quantum computation, have been invented [VC06, Rau05b]. Remarkably, these schemes also work with translationally invariant input states. In [SFW06] it is argued that a circuit model computation can be simulated by a classically controlled QCA, and that such a QCA can be transferred into an autonomous one without external control. A one-dimensional QCA, which is able to simulate all other ones efficiently, is presented in [AFW07], thereby showing that the class of one-dimensional QCAs is intrisically universal. Apart from being a computational model itself, QCAs can also be used for preparing the cluster state, i.e. the resource state for one-way quantum computation, out of a product state [RB01, RB02].

A promising application of quantum cellular automata is quantum simulation of translationally invariant finite range Hamiltonians, e.g. spin chains. As mentioned in the previous Section, the time evolution of such systems is hard to simulate on a classical computer. However, a Trotter decomposition of the time evolution approximately gives a partitioned QCA (for instance, see [Osb06]), thus allowing a simulation by a suitable QCA. The structure of QCAs can also be interpreted as a discrete time analogue of local Hamiltonian dynamics. However, in general, the continuous time evolution is not strictly local in the sense of QCAs, e.g. after an arbitrary small time interval a localized observable can be spread over the whole lattice. Nevertheless, as established by so called Lieb-Robinson bounds there exists an effective lightcone, and outside this lightcone the observables are exponentially damped [LR72, BR97]. This approximate locality is of recent interest in many research groups, which work on the connection of quantum information and many-body systems. Hence, many consequences of Lieb-Robinson bounds are now being established, e.g. the exponential decay of correlations for gapped Hamiltonians [NS06, HK06, NOS06, BHV06, EO06]. The simulation of the continuous time evolution by a QCA, which arises from a Trotter decomposition, seems not optimal, as a rapid switch between the different layers of unitaries is necessary for a good approximation. Finding more suitable approx-

imations would be a promising future project, which will probably make massive use of Lieb-Robinson bounds. Apart from simulation, QCAs can also be used as a tool for variational methods for obtaining ground states [DEO08], or for mapping a Hamiltonian onto a possibly simpler one without changing the spectrum (duality transformation), as demonstrated by Plenio [Ple07]. Note that computational models, similar to those for QCAs, have also been invented for continuous time dynamics, sometimes called Hamiltonian QCAs [VC08, Kay08, NW08].

The expression "quantum cellular automaton" has sometimes been used for the dynamics of a single particle. For instance, the QCA introduced by Grössing and Zeilinger in the late 1980's is a first order approximation of the time evolution of a simple lattice Hamiltonian [GZ88]. Thus, this approximation is local because only nearest neighbor "hopping terms" are involved, but not unitary. Later, Meyer studied local and unitary evolutions, which he also called QCAs [Mey96a]. However, he also introduced interactions between particles, leading to *quantum lattice gas automata*, which can be seen as special QCA evolutions in the up-to-date language.

The dynamics of a single quantum particle in discrete time steps on a lattice is now called *quantum walk* or sometimes *quantum random walk*, as this model is introduced as the quantum analogue of a random walk. In the simplest case, a random walk describes a classical particle (the "walker") on a one dimensional lattice, which decides by a coin toss to move right or left, respectively. A first quantum version of this model was introduced by Aharonov et al. [ADZ93], however the walking direction was determined by a measurement on a spin-1/2-particle, destroying the coherence of the quantum evolution. In the recent model of quantum walks (QWs for short) the coin toss is modeled by a unitary rotation on an internal degree of freedom, which is then followed by a shift step, shifting the particle in dependence on the internal state. Such evolutions first have been discussed by Meyer, who observed that an internal degree of freedom is necessary for a unitary and local evolution [Mey96b]. In the recent notation, QWs have been introduced by Ambainis et al. [ABN$^+$01, NV00] on the line and by Aharonov et al. on general graphs [AAKV01]. An overview can be found in [Kem03].

For a classical random walk, the propagation is diffusive, i.e. the expected distance traveled after t time steps scales as $\sqrt{t}$. In contrast, a QW propagates ballistically (distance proportional to t) due to fully coherent quantum dynamics, similar to a free quantum particle on the line. Therefore, quantum walks are more powerful in search algorithms than their classical counterparts [SKW03, Amb03, Amb04]. However, apart from search algorithms their computational power is limited. For instance, the dynamics can be very well simulated on a classical computer, and the asymptotic probability distribution can even be analytically calculated, e.g. by a group velocity operator [GJS04b].

Here we focus on a different application of quantum walks. As we will see in Chapter 6, QWs are closely related to QCAs, namely they can be interpreted as QCAs, which run with a single particle (or quasi-particle or excitation). In

the other way around, introducing local interactions between quantum walkers passes from QW to QCA dynamics. Any experiment, which is supposed to do a QCA-like transformation, can therefore be run as a QW first. Since QWs are much easier to handle theoretically, even with experimental imperfections, this allows a detailed comparison between experimental and theoretical data. In particular, we hope that decoherence sources can be detected and eliminated with this technique.

Indeed, recently there are many efforts to realize QCA-like transformations experimentally, e.g. with neutral atoms in optical lattices. The atoms are trapped by dipole-interactions in a standing optical wave. They can be transported depending on their spin state [MGW+03a], which directly corresponds to the theoretical conditional shift. The particles interact via cold controlled collisions, which allows to build up entanglement [MGW+03b, WGF+05]. Lately, in the labs of Immanuel Bloch there are also attempts of building interactions by so called "double-well potentials" [FTC+07, BRD+08], where the lasers are tuned such that the potential wells are alternating higher and lower. Effectively, this leads to blockwise nearest neighbor interactions, i.e. a scheme of a partitioned QCA. In the labs of Dieter Meschede realizations of quantum walks with neutral atoms in optical lattices just recently have been produced [KFWM], also based on spin-dependent transport [SDK+04, MAD+06]. A detailed analysis of the experimental data is however left as future work. Quantum walks have also been implemented with high fidelity in waveguide lattices [PLP+08], but it seems not so easy to realize interactions between the photons in such a system.

1.3 Outline and Summary of Results

In this thesis quantum cellular automata and quantum walks are studied both from abstract axiomatic principles and by properties of basic examples. We do not explicitly focus on the computational power, but rather describe fundamental properties and principles, which should simplify further studies and constructions of explicit examples.

All chapters are more or less self-contained with only a small number of cross references. For instance, the index of a QCA, which is introduced in Chapter 3, will be mentioned or calculated for examples in the subsequent chapters. However, these cross references are not fundamental for the understanding of the content of the individual chapters.

In Chapter 2 we will introduce the basic concepts, which will be used throughout the thesis. We start with a short overview on the mathematical framework, especially concerning operator algebras and quasi-local algebras. In Subsection 2.2.1 we describe the basic notions of classical cellular automata and, in particular, the most important results on reversible cellular automata. This allows to observe the common and distinguishing properties of classical and quan-

tum cellular automata, which are formally introduced in Subsection 2.2.2. We describe the recent language of QCAs and show some basic examples and construction methods following the definition of [SW04]. Furthermore, we review the structure theorem of [ANW08], which states that all QCAs can be locally implemented when we allow for an additional ancilla system at each lattice site. In Section 2.3 we introduce the basic notations and results on quantum walks, especially the asymptotic behavior.

The first part of this thesis is concerned with QCAs, starting with an index theory for one-dimensional quantum cellular automata in Chapter 3. We locally quantify the information flow of the dynamics and find that with a suitable normalization this flow is constant along the chain, even without assuming translation invariance. This term is therefore a global, but locally computable, quantity and defined as the index of the quantum cellular automaton. The index of a QCA is a positive rational, which is multiplicative with respect to composition of QCAs. Furthermore, we find that two quantum cellular automata can be continuously deformed into each other, if and only if they have the same index, and we show that quantum cellular automata with trivial index can be locally implemented without any ancillary system. We also show some examples and constructions for indices in higher dimensions for translationally invariant QCAs with special neighborhood schemes.

Chapter 4 is devoted to Clifford QCAs, i.e. QCAs which map Pauli operators to multiples of Pauli operators. These operations can be described in classical terms, in particular, they are induced by classical cellular automata. Therefore, these QCAs do not allow for universal quantum computation. Nevertheless, they can be used to generate entanglement and they allow the study of many aspects, which are hard to determine for general QCAs. We establish their power for entanglement generation by showing that all translationally invariant stabilizer states, i.e. generalized cluster states, can be prepared by a single Clifford QCA time step out of a product state, at least in one lattice dimension or for periodic boundary conditions.

In Chapter 5 we discuss quantum cellular automata, which respect all lattice symmetries, e.g. reflections and discrete rotations, and not only translation symmetry. We find constraints for these additional symmetries and show how the number of parameters, e.g. in interaction terms, can be reduced by these further symmetry conditions.

The second part of this thesis addresses quantum walks. In Chapter 6 we study the connection between quantum walks and quantum cellular automata. We identify QWs with one-particle sectors of QCAs, i.e. a QCA evolution with a single particle as input. Now the question is, how to turn from a given QW to a full QCA rule, allowing arbitrary many particles. If the particles are far apart, the dynamics should, because of locality, still be determined by the quantum walk. However, if the particles meet, we have to introduce some interaction terms. Therefore, we show that every local unitary evolution, i.e. a general QW,

is generated by one-site terms ("coin tosses") and conditional shifts. These operations can be easily extended to full QCA rules by introducing local interactions between the internal states. We use different factorizations to construct different QCA rules, one optimizing the single cell dimension, another one optimizing the neighborhood scheme.

In Chapter 7 we introduce an index theory for quantum walks, similar to the case of QCAs in Chapter 3. The results are indeed very similar although the mathematical tools to achieve them are quite different. For QWs the index corresponds more to a quantification of the mean velocity rather than the information flow. However, this quantity is also constant along the line without assuming translation symmetry. In contrast to the case of QCAs, the index of a QW is an integer, which is additive with respect to composition of QWs. The connectivity of QWs with the same index is established analogously to the QCA case. In the translationally invariant case, we can connect, with the help of the factorization presented in Chapter 6, the index with the determinant of the Fourier transform of the walk and also with the winding number of the eigenvalues. For higher lattice dimensions most results can be generalized, if we assume translation invariance.

Finally, we discuss noisy quantum walks in Chapter 8. Indeed, experimental imperfections destroy the coherence of the quantum evolution, and let it pass to classical behavior for long times. As usual, such decoherence effects can be modeled as a reversible evolution on a larger system containing a suitable environment, leading to irreversible dynamics on the observed subsystem. We first describe the general structure of such local and translationally invariant transformations. Further, we discuss the asymptotic behavior of the probability distribution, e.g. we study whether we get classical-like, diffusive behavior or keep quantum-like, ballistic propagation behavior. For most decoherent QWs we find indeed classical-like behavior. We establish perturbation theory techniques to calculate analytically the variance of the asymptotic probability distribution in dependence of the noise parameters. Furthermore, we show how to model special sources of decoherence, e.g. fluctuating coin parameters.

Chapter 2

Basic Concepts

This Chapter is supposed to introduce the basic notions, which will be used throughout the thesis. In particular, the mathematical framework for a general theory of quantum cellular automata will be provided. Of course, here we can only give a brief overview on the mathematical background and detailed proofs are generally omitted for the sake of brevity.

We start in Section 2.1 by briefly describing the structure of operator algebras, which are associated with quantum systems. Especially, we introduce the notion of quasi-local algebras, which provide the basic description of infinite spin chains (or higher dimensional analogues). These systems will be the basis of a concise definition of quantum cellular automata as discussed in Subsection 2.2.2. However, before introducing the notion of quantum cellular automata we will briefly review the theory of classical cellular automata in Subsection 2.2.1. Finally, quantum walks will be introduced in Section 2.3.

More specialized mathematical tools, which are only relevant in certain chapters, will be described in the appendix. Especially, the concept of support algebras is provided in Appendix A. Some rather technical lemmata are given in Appendix B.

2.1 Mathematical Preliminaries

2.1.1 Quantum Systems

In this Subsection we will provide the basic description of quantum systems. Usually, a quantum system is identified with some Hilbert space $\mathcal{H}$, e.g. $\mathcal{H} = \mathbb{C}^d$ for a d-level system. From the physical point of view the operations on this space are in many applications more important than the space itself. All relevant operations can be described by linear transformations, e.g. by $d \times d$-matrices for a d-level system. This operational description is best phrased in terms of C^*-algebras, i.e. by its observable algebra, which gives a unified approach to both

quantum and classical systems, or hybrids composed of a classical and a quantum part. For this operator algebraic approach several textbooks are worth reading, especially we refer to the books by Bratteli and Robinson [BR87, BR97].

The properties of an abstract C^*-algebra are defined analogous to the properties of the algebra of bounded operators $\mathcal{B}(\mathcal{H})$ on some Hilbert space. In particular, every such algebra is a C^*-algebra and every abstract C^*-algebra is isomorphic to a norm-closed subalgebra of $\mathcal{B}(\mathcal{H})$ for a suitable Hilbert space $\mathcal{H}$.

A C^*-algebra $\mathcal{A}$ is a vector space over the complex field $\mathbb{C}$, which is endowed with a (not necessarily commutative) product and also closed under products, i.e. for $A, B \in \mathcal{A}$ we have $AB \in \mathcal{A}$. Further, $\mathcal{A}$ is closed under an *adjoint* operation[1] (or *star* operation or *involution*) $\mathcal{A} \ni A \mapsto A^* \in \mathcal{A}$, which fulfils $A^{**} = A$, $(\alpha A + \beta B)^* = \overline{\alpha} A^* + \overline{\beta} B^*$ and $(AB)^* = B^* A^*$ for all $A, B \in \mathcal{A}\,, \alpha, \beta \in \mathbb{C}$.

The *norm* $\|\cdot\|$ on $\mathcal{A}$ fulfils all usual properties of any norm on a vector space, i.e., $\|A\| = 0$ implies $A = 0$, $\|\alpha A\| = |\alpha| \|A\|$ and the triangle inequality $\|A + B\| \leq \|A\| + \|B\|$ holds for all $A, B \in \mathcal{A}$, $\alpha \in \mathbb{C}$. Further, the product inequality $\|AB\| \leq \|A\| \|B\|$ must be satisfied, which indicates $\mathcal{A}$ as a Banach algebra. Finally, the C^*-condition $\|A^* A\| = \|A\|^2$ for all $A \in \mathcal{A}$ is required.

An *identity* $\mathbb{1} \in \mathcal{A}$ is an element, which fulfills $\mathbb{1} A = A = A \mathbb{1}$ for all $A \in \mathcal{A}$. A C^*-algebra is not necessarily equipped with an identity, but in our cases we will always have such an element.

If $\mathcal{A}$ is identified as a subalgebra of $\mathcal{B}(\mathcal{H})$ the involution is defined such that $\langle \phi, A\psi \rangle = \langle A^* \phi, \psi \rangle$ holds for all $\phi, \psi \in \mathcal{H}$, where $\langle \cdot, \cdot \rangle$ denotes the scalar product. The norm corresponds to the usual operator norm $\|A\| = \sup_{\psi \in \mathcal{H}, \|\psi\| = 1} \|A\psi\|$, where the norm on the Hilbert space level is given by $\|\psi\|^2 = \langle \psi, \psi \rangle$ for $\psi \in \mathcal{H}$.

As already mentioned, the product in a C^*-algebra $\mathcal{A}$ is in general not commutative, but there may be some elements in the algebra, which commute with all the others. This set is denoted by the center

$$\mathcal{Z}(\mathcal{A}) = \{A \in \mathcal{A} |\, AB = BA \;\; \forall B \in \mathcal{A}\}\,, \tag{2.1}$$

which is itself an algebra. The center helps to analyze the structure of the algebra. For instance, if $\mathcal{Z}(\mathcal{A}) = \mathcal{A}$ holds, the algebra is *commutative* or *abelian*.

Furthermore, for a C^*-algebra $\mathcal{A} \subset \mathcal{B}(\mathcal{H})$ we have the *commutant* defined by

$$\mathcal{A}' = \{B \in \mathcal{B}(\mathcal{H}) |\, AB = BA \;\; \forall A \in \mathcal{A}\}\,. \tag{2.2}$$

The commutant is therefore a subalgebra of $\mathcal{B}(\mathcal{H})$ and the center is in this case given by $\mathcal{Z}(\mathcal{A}) = \mathcal{A} \cap \mathcal{A}'$. In the extremal case $\mathcal{A} = \mathcal{B}(\mathcal{H})$ we clearly have $\mathcal{A}' = \mathbb{C}\mathbb{1}$, i.e. the commutant is trivial, which refers to a full quantum system.

For many purposes we are concerned with finite dimensional systems, i.e., $\mathcal{A}$ is identified with a subset of $\mathcal{M}_d$, the algebra of complex $d \times d$-matrices. If the commutant is trivial, $\mathcal{A}$ is given by $\mathcal{M}_d$ itself and describes a d-level quantum

[1] Note that in physics the notation $A^\dagger$ is also common.

system. In the other extreme $\mathcal{A}$ is abelian, which means that $\mathcal{A}$ is in a suitable basis given by a set of diagonal matrices. In information theory such an algebra describes a classical system. Of course, there are also examples of C^*-algebras between these extremal cases, e.g. a direct sum $\mathcal{M}_{d_1} \oplus \mathcal{M}_{d_2} \subset \mathcal{M}_{d_1+d_2}$ of matrix algebras (this describes a hybrid of a quantum system and a classical system). However, the following Proposition states that this is already the only possible structure of a finite dimensional C^*-algebra.

Proposition 2.1 *Every finite dimensional C^*-algebra $\mathcal{A}$ is isomorphic to a direct sum of full matrix algebras, i.e., there exist $d_1, \ldots, d_n \in \mathbb{N}$ such that*

$$\mathcal{A} \cong \bigoplus_{j=1}^{n} \mathcal{M}_{d_j} \,. \tag{2.3}$$

In a quantum computing scheme usually many quantum systems are involved. Therefore, we need to compose quantum systems, which is done by a tensor product. On the algebraic level this is given by

$$\mathcal{A}_1 \otimes \mathcal{A}_2 = \mathrm{span}\{A_1 \otimes A_2 |\, A_1 \in \mathcal{A}_1,\, A_2 \in \mathcal{A}_2\}\,,$$

which defines according to the relations $(A_1 \otimes A_2)^* = A_1^* \otimes A_2^*$ and $(A_1 \otimes A_2)(B_1 \otimes B_2) = A_1 B_1 \otimes A_2 B_2$ again a C^*-algebra. For full quantum systems $\mathcal{A}_1 = \mathcal{B}(\mathcal{H}_1)$ and $\mathcal{A}_2 = \mathcal{B}(\mathcal{H}_2)$ the tensor product corresponds to taking the tensor products of the Hilbert spaces, i.e. $\mathcal{B}(\mathcal{H}_1) \otimes \mathcal{B}(\mathcal{H}_2) \cong \mathcal{B}(\mathcal{H}_1 \otimes \mathcal{H}_2)$. For n instead of two systems all relations can be straightforwardly generalized, but for infinitely many systems the tensor product causes some trouble. How to circumvent this, will be described in the following Subsection.

2.1.2 Quasi-local Algebras

The underlying system of a quantum cellular automaton is a lattice of finite dimensional quantum systems, i.e., to each lattice point a quantum system is assigned and the overall system is the tensor product over all lattice points. Since we want to tackle also infinite lattices like $\mathbb{Z}^s$, this leads to an infinite tensor product. This Subsection is devoted to a rigorous definition of such a system, which is also used in statistical mechanics of quantum spin systems (see [BR87, BR97]).

Of course, we can assign a Hilbert space $\mathcal{H}_x \cong \mathbb{C}^d$ to each lattice point $x \in \mathbb{Z}^s$. Let us first see, whether we can make sense of the tensor product "$\mathcal{H} = \bigotimes_{x\in\mathbb{Z}^s} \mathcal{H}_x$". Fix therefore two vectors $\phi, \psi \in \mathbb{C}^d$. The scalar product in $\mathcal{H}$ for the infinite product vectors then gets $\langle \phi^{\otimes \mathbb{Z}^s}, \psi^{\otimes \mathbb{Z}^s} \rangle_{\mathcal{H}} = \prod_{x\in\mathbb{Z}^s} \langle \phi, \psi \rangle_{\mathcal{H}_x}$, i.e. an infinite product, which does not exist in general (take e.g. $\langle \phi, \psi \rangle = e^{i\lambda}$ for some $\lambda \neq 0$). Hence, there is no scalar product in $\mathcal{H}$, which shows that this approach does not work. One could remove the convergence problem by demanding that

all states agree with a "quiescent" state on cells far outside. For classical systems this corresponds to finite configurations, which are also discussed for cellular automata. Nevertheless, this approach would not allow translationally invariant states apart from the one, which is quiescent everywhere. Further, the locality condition on quantum cellular automata is not easy to handle in this way, which suggests an alternative approach.

Let us therefore go to an operator algebraic approach. The observable algebra at lattice point $x \in \mathbb{Z}^s$ is given by $\mathcal{A}_x = \mathcal{B}(\mathcal{H}_x) \cong \mathcal{M}_{d(x)}$, i.e., we allow the single cell dimension to depend on x (of course, all $d(x)$ should be finite and uniformly bounded). For a finite subset $\Lambda \subset \mathbb{Z}^s$ we identify the observable algebra by the tensor product $\mathcal{A}(\Lambda) = \bigotimes_{x\in\Lambda} \mathcal{A}_x$. For finite sets $\Lambda_1 \subset \Lambda_2$ the algebra $\mathcal{A}(\Lambda_1)$ can be identified as subalgebra of $\mathcal{A}(\Lambda_2)$ by tensoring with the identity $\mathbb{1}^{\Lambda_2\setminus\Lambda_1}$, i.e. $\mathcal{A}(\Lambda_1) \cong \mathcal{A}(\Lambda_1) \otimes \mathbb{1}^{\Lambda_2\setminus\Lambda_1} \subset \mathcal{A}(\Lambda_2)$. This identification also makes the product A_1A_2 with $A_j \in \mathcal{A}(\Lambda_j)$ a well-defined element of $\mathcal{A}(\Lambda_1 \cup \Lambda_2)$. Since tensoring with the identity does not change the norm, we get a normed algebra of local observables. The completion is then the *quasi-local algebra*

$$\mathcal{A}(\mathbb{Z}^s) := \overline{\bigcup_{\substack{\Lambda\subset\mathbb{Z}^s \\ finite}} \mathcal{A}(\Lambda)}\,. \tag{2.4}$$

In particular, every element of $\mathcal{A}(\mathbb{Z}^s)$ can be approximated by strictly local observables, which is an important fact for the existence of several dynamical systems, e.g. a quantum cellular automaton defined by commuting unitaries (see Subsection 2.2.2). An observable is called localized on Λ, if it is an element of $\mathcal{A}(\Lambda)$.

In Chapter 3 we will indeed be concerned with systems where the local cell dimension $d(x)$ is allowed to depend on x. To emphasize this dependence, the quasi-local algebra will there also be denoted by $\{\mathcal{A}_x\}_{x\in\mathbb{Z}} = \mathcal{A}(\mathbb{Z})$ and referred to as cell structure.

However, in many cases we have that $d(x) \equiv d$ does not depend on x. In this case we can define the shift operation τ^x for each $x \in \mathbb{Z}^s$ by the canonical isomorphism from each $\mathcal{A}_y$ to $\mathcal{A}_{x+y}$. Extending this to local observables gives isomorphisms $\mathcal{A}(\Lambda) \to \mathcal{A}(\Lambda+x)$, where we use the notation $\Lambda+x = \{y+x|\, y \in \Lambda\}$, which we also use for two subsets $\Lambda_1 + \Lambda_2 = \{x_1 + x_2|\, x_j \in \Lambda_j\}$. The set of shift operations defines a representation of the group $(\mathbb{Z}^s, +)$ on the quasi-local algebra $\mathcal{A}(\mathbb{Z}^s)$, i.e., we have $\tau^{x+y} = \tau^x \circ \tau^y$ for all $x, y \in \mathbb{Z}^s$.

2.1.3 States and Transformations

Let the quantum system be described by some observable algebra $\mathcal{A}$. A *state* of the system describes a preparation, and a measurement of an observable $A \in \mathcal{A}$ on a system in a state ω gives a distribution (by repeating the measurement) with expectation value $\omega(A)$, i.e., the state is described by a linear functional

$\omega : \mathcal{A} \to \mathbb{C}$. Furthermore, a state ω has to be positive ($\omega(A^*A) \geq 0$ for all $A \in \mathcal{A}$) and normalized ($\omega(\mathbb{1}) = 1$). The space of linear functionals is called the dual space $\mathcal{A}^*$ of $\mathcal{A}$, and the set of all states in $\mathcal{A}^*$ is convex, i.e., $\omega = \lambda\omega_1 + (1-\lambda)\omega_2$ is a state for all $0 \leq \lambda \leq 1$ whenever ω_1 and ω_2 are states. A state ω which can not be decomposed in this way (unless $\omega = \omega_1 = \omega_2$) is called a *pure state*.

A state ω on a composed system $\mathcal{A}_1 \otimes \mathcal{A}_2$ is called *separable* or *classically correlated*, if it can be decomposed as $\omega = \sum_k \lambda_k \omega_k^{(1)} \otimes \omega_k^{(2)}$, where the $\omega_k^{(j)}$ are states on $\mathcal{A}_j$ and $\sum_k \lambda_k = 1$. A state, which does not allow such a decomposition, is called *entangled*. A state ω on the quasi-local algebra $\mathcal{A}(\mathbb{Z}^s)$ is called *translationally invariant* if $\omega(\tau^x A) = \omega(A)$ for all $A \in \mathcal{A}(\mathbb{Z}^s)$ holds.

Usually, a state underlies some transformation before the measurement is executed. This can be the free time evolution of the system, but the transformation may also contain (usually unintentional) interactions with the environment. In general, such transformations can also connect different systems $\mathcal{A}$ and $\mathcal{B}$. Nevertheless, the transformation has to map states of $\mathcal{A}$ onto states of $\mathcal{B}$ and all such transformations are called *channels*. For computing the expectation value after applying some channel, one can transform the initial preparation, i.e. the state (Schödinger picture), or one can transform the observable to be measured (Heisenberg picture). In the first case the channel is described by a linear map $T_* : \mathcal{B}^* \to \mathcal{A}^*$ between the dual spaces, in the second case by a linear transformation $T : \mathcal{A} \to \mathcal{B}$ between the observable algebras. Of course, the transformations can only be equivalent, if the expectation value is the same in both cases, i.e., we must have $(T_*\omega)(A) = \omega(T(A))$ for all $A \in \mathcal{A}$. Here we will mainly work in the Heisenberg picture. The property of T_* mapping states to states, implies that T has to be *completely positive* and *unital*. Positivity means that T maps positive operators to positive operators, and complete positivity means that this is true for $T \otimes \mathrm{id}_n$ on $\mathcal{A} \otimes \mathcal{M}_n$ for all $n \in \mathbb{N}$, i.e. if there is an "innocent bystander". T is called unital or unit-preserving if $T(\mathbb{1}_{\mathcal{A}}) = \mathbb{1}_{\mathcal{B}}$ holds.

In most of the chapters we will be concerned with reversible transformations. On the Hilbert space level an invertible transformation is just given by a unitary operator $U \in \mathcal{B}(\mathcal{H})$, i.e. $UU^* = U^*U = \mathbb{1}$. An observable $A \in \mathcal{A} = \mathcal{B}(\mathcal{H})$ is transformed by the conjugation with this unitary, i.e., $T(A) = U^*AU$. It is easy to see that such a transformation conserves all the algebraic structures of the observable algebra, for instance, we have $T(A^*) = T(A)^*$ and $T(AB) = T(A)T(B)$ for all $A, B \in \mathcal{A}$. Such a structure preserving map is called a *homomorphism*, and if it is also bijective it is called an *automorphism*. Automorphisms are exactly the reversible transformations on an observable algebra $\mathcal{A}$, even when an underlying Hilbert space does not exist. However, on a finite dimensional observable algebra $\mathcal{A}$ an automorphism is always implemented by a unitary operator $U \in \mathcal{A}$.

In Chapter 8 we will study decoherent quantum walks, i.e. irreversible transformations. However, the famous Stinespring representation theorem states that an irreversible transformation can always be handled as a reversible one on a larger system (see for instance the book by Paulsen [Pau02]). The version pre-

sented here is a special case where the input system is a pure quantum system, i.e. of the type $\mathcal{B}(\mathcal{H})$.

Theorem 2.2 (Stinespring Dilation) *Let $T : \mathcal{B}(\mathcal{H}_1) \to \mathcal{B}(\mathcal{H}_2)$ be a completely positive and unital map. Then there exists a Hilbert space $\mathcal{K}$ and an isometry $V : \mathcal{H}_2 \to \mathcal{H}_1 \otimes \mathcal{K}$, i.e $V^*V = \mathbb{1}_{\mathcal{H}_2}$, such that*

$$T(A) = V^*(A \otimes \mathbb{1}_{\mathcal{K}})V \quad \forall A \in \mathcal{B}(\mathcal{H}_1) \tag{2.5}$$

holds.

By introducing a basis in the ancillary space $\mathcal{K}$ one obtains the Kraus form of a channel [Kra83].

Corollary 2.3 (Kraus representation) *For every completely positive and unital map $T : \mathcal{B}(\mathcal{H}_1) \to \mathcal{B}(\mathcal{H}_2)$ there exist operators $K_j : \mathcal{H}_2 \to \mathcal{H}_1$ with $\sum_j K_j^* K_j = \mathbb{1}_{\mathcal{H}_1}$ such that*

$$T(A) = \sum_j K_j^* A K_j \quad \forall A \in \mathcal{B}(\mathcal{H}_1)\,. \tag{2.6}$$

2.2 Quantum Cellular Automata

Before we will introduce quantum cellular automata and describe their basic properties, we give a short overview on classical cellular automata. In particular, we will state the most important results on reversible cellular automata since we will deal mainly with reversible transformations in the quantum case, too. Some properties of classical cellular automata are also worth to be studied in the quantum case. Remarkably, some results turn out to have a direct analog for quantum cellular automata, whereas some properties are strikingly different.

2.2.1 Classical Cellular Automata

Cellular automaton structures are known since the 1940's. Stanisław Ulam was working on models of crystal growth, while John von Neumann, his colleague at Los Alamos, was trying to find self-replicating systems, i.e, a process by which one thing produces a copy of itself. Ulam suggested to develop an abstract model similar to those he used for studying crystal growth, which helped von Neumann to invent his so called universal constructor [vN66], which is a special cellular automaton on a two dimensional lattice with 29 states per cell but only a small neighborhood scheme (see Figure 2.1).

The most popular example of a cellular automaton is probably John Conway's "Game of Life" invented in the 1970's [BCG82]. This is also a two dimensional cellular automaton but only with two states per cell and Moore neighborhood (see Figure 2.1). The states are labeled with "live" or "dead", which allows a

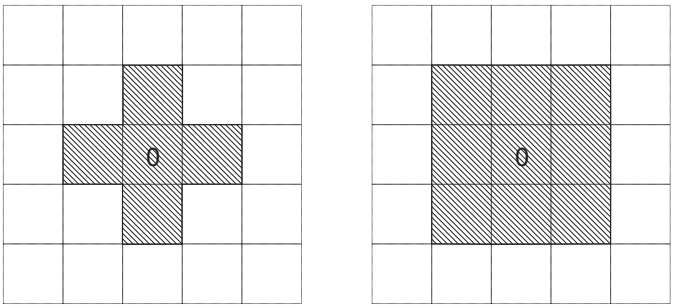

Figure 2.1: *Left: von Neumann neighborhood scheme. Right: Moore neighborhood scheme.*

simple description of the evolution: a live cell with more than three live neighbors dies (because of overcrowding), a live cell with less than two live neighbors dies (because of underpopulation), and a dead cell with exactly three live neighbors becomes live. Although these rules are rather simple, the cellular automaton allows for many complex phenomena, such as the existence of gliders, i.e., configurations which travel without changing their shape, and it has the same computational power as a universal Turing machine.

Apart from developing cellular automaton models for specified purposes, the general structure of cellular automata has also been widely studied. For instance, there are attempts to characterize and classify them by their space-time diagrams, ultimately leading to a rather thick book by Wolfram [Wol02]. Surprisingly, he states that the behavior of a cellular automaton may be complex enough to model the whole universe, an idea which led him title the book with "A new kind of science". Since the mathematical details of such an approach are not really clear, we will not further follow this direction.

Since we deal mostly with reversible quantum cellular automata, the theory of reversible classical cellular automata is more interesting for us. Different to the quantum version, for which a satisfying theory is up to now only available in the reversible case, reversibility in classical cellular automata was developed out of the general theory. We will briefly review the most important results on reversible cellular automata because for some of them we will find analogous results in the quantum case, but first we will give a formal definition of cellular automata.

The underlying structure of a cellular automaton consists of a lattice $\mathbb{Z}^s$ and a finite set A of symbols, e.g. $\{0, 1\}$ in the simplest case, which is associated to each lattice point. The number of symbols in A is also referred to as the (local) cell dimension. A configuration c assigns some symbol of A to each lattice point, i.e., it can be identified with a mapping $c : \mathbb{Z}^s \to A$. The space of all configurations will be denoted by $A^{\mathbb{Z}^s}$. A cellular automaton is defined by a finite subset $\mathcal{N} \subset \mathbb{Z}^s$, the neighborhood scheme, and a mapping $t_0 : A^{\mathcal{N}} \to A$, the local transition rule.

The global rule $t : A^{\mathbb{Z}^s} \to A^{\mathbb{Z}^s}$ transforms a configuration by applying the local rule in parallel to all cells, i.e. we have $t(c)(x) = t_0(\{c(y)|y \in x + \mathcal{N}\})$.

From this definition some problems concerning invertibility are apparent, mainly because a cellular automaton is described in terms of a local rule, but invertibility is a property of the global mapping. This gives rise to several questions: If the global rule is invertible, is then the inverse also a local mapping, i.e. a cellular automaton? If this is true, how is the neighborhood scheme of the inverse related to the original one? Is it possible to decide from the local rule, whether the cellular automaton is invertible? If this is true, can one efficiently compute the local rule of the inverse automaton from the local rule?

For a long time only simple procedures for constructing invertible cellular automata have been known, and therefore it was unclear whether they are capable of doing nontrivial things, e.g. modeling of microscopic reversible phenomena. Aside from explicit examples, the general study of invertibility in cellular automata systems raised the above questions, which have been answered over the years. In the following paragraphs we will state the most important results. Of course, this is only a little excerpt out of the achieved results without going into technical details. For a nice, although a little dated review on invertible cellular automata see the article by Toffoli and Margolus [TM90]. More recent reviews can be found in [Kar05a, Kar05b].

In 1972 Richardson found that locality is equivalent to continuity in a certain topology on the space of configurations, namely the product topology, which enabled him to prove the following result.

Theorem 2.4 ([Ric72]) *If a cellular automaton is injective, then it is also surjective and its inverse is a local transformation, i.e. a cellular automaton.*

Although this is a very fundamental and important result, Richardson does not give any method to construct the inverse local rule. Also, his techniques do not help to answer, whether invertibility of a cellular automaton can be decided by local data. But at the same time, this question was answered by Amoroso and Patt, at least in one lattice dimension.

Theorem 2.5 ([AP72]) *Given an arbitrary one-dimensional cellular automaton in terms of a local rule, there is an effective procedure to decide whether this automaton is invertible or not.*

This decision procedure mainly works because there exists a bound on the neighborhood of the inverse automaton, which depends on the neighborhood and the cell dimension of the forward automaton [CK05]. This gives a finite number of possible inverse local rules, which can easily be checked (by composing with the forward rule and looking at the image of a single cell), whether they correspond indeed to the inverse rule or not. Quite a while it was not clear whether such a result is also true for higher dimensions, until Kari disproved it [Kar90]. In

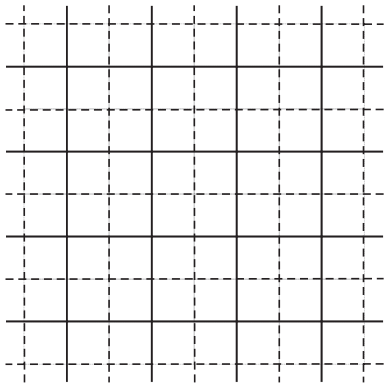

Figure 2.2: *Different tilings of the infinite lattice with* 2×2*-blocks of cells.*

particular, this implies that there is no upper bound on the inverse neighborhood in higher dimensions.

Theorem 2.6 ([Kar90]) *There is no procedure, which effectively decides whether an arbitrary two-dimensional cellular automaton is invertible or not.*

A powerful construction scheme for reversible cellular automata was introduced by Margolus [Mar84]. In his scheme neighboring cells are grouped to blocks, where all these different blocks do not overlap (see Figure 2.2). Now to each single block the same transformation is applied, and the global mapping is invertible if and only if this block transformation is invertible. This fact is one of the main purposes of the construction because invertibility can be checked by local data. Furthermore, these transformations allow for a block-wise implementation, which is strictly local, i.e. without any overlapping transformations. Of course, a single step of such a block transformation will not be very interesting, but alternating between different block structures and transformations allows for a versatile construction of reversible cellular automata.

Indeed all reversible cellular automata can be essentially implemented in this way. Kari showed that up to some shift-like transformation every reversible cellular automaton can be implemented by a sequence of block permutations, at least in one and two lattice dimensions [Kar96]. These shift-like transformations are so called conditional shifts, i.e. maps which translate a symbol by some lattice vector, where this lattice vector depends on the given symbol. Durand-Lose achieves an implementation in terms of block transformations by enlarging the local cell dimension [DL95, DL01].

It may seem that these results limit the computational capabilities of re-

versible cellular automata, but as was shown by Toffoli every computation universal cellular automaton can be imbedded into an invertible one by allowing one additional lattice dimension [Tof77]. Furthermore, it has been shown that also one lattice dimension suffices to construct a reversible computation universal cellular automaton [MH89].

2.2.2 Basics of Quantum Cellular Automata

Since the beginning of quantum information theory and quantum computing there have been several attempts of transferring cellular automata structures to the quantum regime. The basic idea is very simple: just replace the set of symbols by a finite quantum system and the global rule by a completely positive map, which should act locally in a certain sense. But there are some serious problems when one wants to turn this idea into a rigorous mathematical formulation, and many attempts of defining quantum cellular automata have not been really satisfying (see Section V. of [SW04] for detailed comments on alternative approaches).

A principal task is already the formulation of the quantum system itself, without the dynamics, since infinitely many quantum systems have to be composed. As argued in Subsection 2.1.2, a formulation in terms of Hilbert spaces seems not appropriate and defining the system by a C^*-algebra is more suitable. Therefore, we identify the quantum system with a quasi-local algebra $\mathcal{A}(\mathbb{Z}^s)$ over a lattice $\mathbb{Z}^s$ as introduced in Subsection 2.1.2, where the algebra of a single cell describes a d-level quantum system, i.e. $\mathcal{A}_x \cong \mathcal{M}_d$. Since the quasi-local algebra describes the observables of the system rather than the states, this suggests to formulate the dynamics in the Heisenberg picture rather than in the Schrödinger picture. This approach also solves the second challenging task, namely a suitable formulation of locality because the notion of localized observables is contained in the structure of quasi-local algebras whereas states are always a global concept, which do in general not allow a complete local description. A plausible way of formulating the locality condition is that local observables are mapped to local observables, possibly localized on a slightly larger region. This formulation is equivalent to a no-signalling condition, meaning that in one time step no signals can be sent from far apart constituents.

Another challenging task is to describe how the propagation of information is managed. In general, the content of a single cell at some time t should influence the information in several cells at time $t + 1$. In a classical system this can be managed by copying the information and transfering the copies to the cells in the neighborhood. Since in a quantum system a no-cloning constraint holds, an analogous procedure is not possible for the quantum case. This seems to be a rather weird problem, which is up to now only solved in the reversible case.

All these ideas have led to the following definition of (reversible) quantum cellular automata [SW04].

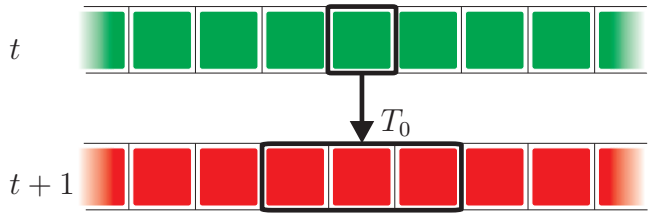

Figure 2.3: *Local rule of the global time step.*

Definition 2.7 *A* **reversible quantum cellular automaton (QCA)** *with neighborhood scheme $\mathcal{N} \subset \mathbb{Z}^s$ is a unital homomorphism $T : \mathcal{A}(\mathbb{Z}^s) \to \mathcal{A}(\mathbb{Z}^s)$ of the quasi-local algebra, which commutes with the lattice translations τ^x and fulfills the locality condition $T(\mathcal{A}(\Lambda)) \subset \mathcal{A}(\Lambda + \mathcal{N})$ for all finite regions $\Lambda \subset \mathbb{Z}^s$. The* **local rule** *$T_0$ of a quantum cellular automaton T is defined by the restriction to the one-site algebra, i.e., $T_0 = T|_{\mathcal{A}_0} : \mathcal{A}_0 \to \mathcal{A}(\mathcal{N})$.*

Note that invertibility is not explicitly postulated in this Definition since this would require the global rule to be an automorphism and not only a homomorphism. But as we will state below, invertibility follows from the Wrapping Lemma 2.9. Remarkably, this only holds in the translationally invariant case, and when we study QCAs without translation symmetry in Chapter 3, we have to insist on the automorphism condition.

In the classical case, we first defined a local rule from which we constructed a global rule. In the quantum case, it is more the other way round: we first define the global rule from which a local rule can be obtained. Now the question is, whether it is possible to construct a global rule of a quantum cellular automaton out of a local one, or which conditions suitable mappings have to fulfill for being a valid local rule. Explicitly, given a mapping $T_0 : \mathcal{A}_0 \to \mathcal{A}(\mathcal{N})$ this map should be a homomorphism since it is supposed to be a restriction of a global homomorphism. Furthermore, by translation invariance this mapping can be transferred to any single cell by $T_x = \tau^x \circ T_0 \circ \tau^{-x} : \mathcal{A}_x \to \mathcal{A}(\mathcal{N} + x)$, which allows to compute the image of any local observable. Furthermore, let us look at observables $A_x \in \mathcal{A}_x, A_y \in \mathcal{A}_y$ which are localized on different cells and therefore commute. Their images $T_x(A_x)$ and $T_y(A_y)$ possibly overlap on some cells, but since the global homomorphism conserves the commutation relations these images also have to commute. In total, the following Lemma is obtained (see [SW04] for a detailed proof).

Lemma 2.8 ([SW04])

- *The global rule of a QCA T is uniquely determined by the local rule T_0.*
- *A homomorphism $T_0 : \mathcal{A}_0 \to \mathcal{A}(\mathcal{N})$ is a transition rule of a quantum cel-*

lular automaton if and only if for all $0 \neq x \in \mathbb{Z}^s$ *the algebras* $T_0(\mathcal{A}_0)$ *and* $\tau^x T_0(\mathcal{A}_0)$ *commute elementwise.*

In some cases it would be nice to pass from an infinite system to a finite one, e.g. by assuming periodic boundary conditions. Formally, this is equivalent to turning from an infinite lattice $\mathbb{Z}^s$ to a s-dimensional torus $\mathbb{T}^s$. For a verification of a local mapping to be a local rule according to the previous Lemma, this does not cause any problems since only finitely many cells are essentially involved in checking the commutation relations. In detail, the algebras $T_0(\mathcal{A}_0)$ and $\tau^x T_0(\mathcal{A}_0)$ commute trivially for all but finitely many x because of different localization regions. The only condition on the boundary conditions is that $\mathbb{T}^s$ is not too small compared to the neighborhood scheme. Otherwise, there could occur overlaps of $\mathcal{N}$ and $\mathcal{N} + x$ around the torus, which do not occur in an infinite plane. Neighborhood schemes in $\mathbb{T}^s$, which do not produce such weird overlaps, are called regular.

Lemma 2.9 (Wrapping Lemma [SW04]) *The QCA rules on a torus* $\mathbb{T}^s$ *with respect to a regular neighborhood scheme* $\mathcal{N}$ *are in exact correspondence to QCA rules on* $\mathbb{Z}^s$ *with the same neighborhood scheme.*

This Lemma enables us to consider any QCA on a finite lattice and thereby on a finite quantum system. Since a unital homomorphism on a finite dimensional system is always implemented by a unitary matrix, every QCA according to Definition 2.7 is indeed invertible on every finite torus and therefore also on $\mathcal{A}(\mathbb{Z}^s)$.

As mentioned in the previous Subsection, in the classical reversible case there exists in general no upper bound on the neighborhood scheme of the inverse automaton. Surprisingly, this is much easier in the quantum case. The neighborhood scheme can be formulated in algebraic terms, e.g. in commutation conditions, which helps to find that the inverse neighborhood is in the most intuitive way connected to the forward neighborhood. For any QCA T we define the minimal neighborhood scheme at some point x by

$$\mathcal{N}(x) = \{y | [T(\mathcal{A}_x), \mathcal{A}_y] \neq 0\}\,, \tag{2.7}$$

which is, at least in the translationally invariant case, of the form $\mathcal{N}(0) + x$. Of course, any finite set containing this $\mathcal{N}$ is also a satisfying neighborhood scheme according to Definition 2.7, but Eq. (2.7) gives exactly the smallest one. Using that a homomorphism conserves the commutation relations, we find for the minimal neighborhood of the inverse QCA

$$\begin{aligned} \mathcal{N}^{-1}(x) &= \{y |\, [T^{-1}(\mathcal{A}_x), \mathcal{A}_y] \neq 0\} \\ &= \{y |\, [\mathcal{A}_x, T(\mathcal{A}_y)] \neq 0\} = \{y |\, x \in \mathcal{N}(y)\}\,, \end{aligned}$$

and, by setting $x = 0$, we find

$$\mathcal{N}^{-1} = -\mathcal{N}\,. \tag{2.8}$$

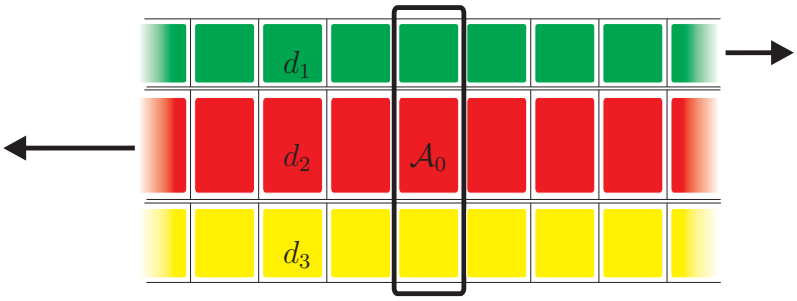

Figure 2.4: *Conditional shift on a system with single cell algebra* $\mathcal{A}_0 = \mathcal{M}_{d_1} \otimes \mathcal{M}_{d_2} \otimes \mathcal{M}_{d_3}$. *The first system is shifted one position to the right, the second system two positions to the left and the third system is unchanged.*

Basic construction schemes

Up to now we have only defined quantum cellular automata in abstract algebraic terms. The existence of nontrivial QCAs is not guaranteed at this point. Therefore, we give some examples of construction schemes, which demonstrate the versatile possibilities of building QCAs and which will be used throughout this thesis in different contexts.

- **Conditional (or partial) shifts:** The most trivial examples of QCAs are simply the shifts τ^x for some $x \in \mathbb{Z}^s$. These are QCAs with a single cell neighborhood scheme and therefore rather uninteresting, e.g. most times it even suffices to analyze the structure of a QCA up to such global shift. Slightly more interesting structures arise by combining these shifts. For instance, if the single cell system is composed into a subcell structure by a tensor product $\mathcal{A}_x = \mathcal{M}_{d_1} \otimes \ldots \otimes \mathcal{M}_{d_n}$, one can apply different shifts to each tensor factor (see Figure 2.4). Clearly, the content of the subcells is also just shifted by some lattice vector x, but this vector x now depends on which subcell is affected. Such operations alone are also not really powerful, but by alternating with other simple QCAs, e.g. single site operations, interesting examples arise, e.g. the lattice gas constructions studied in Chapter 6.

- **Commuting unitaries:** Another simple example of a QCA is to apply the same unitary transformation to each single cell. But an overall unitary operator is ill-defined, similar to the Hilbert space of the system. For instance, this could lead to an infinite product of phases which does clearly not exist. In the following we show how to handle this even for more general unitaries.

  Consider some local unitary operator $U_0 \in \mathcal{A}(\mathcal{L})$, which commutes with all its translates $U_x = \tau^x U_0$ up to a phase, i.e., there are $\xi_x \in \mathbb{C}$ with $|\xi_x| = 1$

such that

$$U_x U_y = \xi_{x-y} U_y U_x \tag{2.9}$$

holds. Formally, we would like to define a unitary operator

$$\text{“}U = \prod_{x \in \mathbb{Z}^s} U_x \text{”}\,, \tag{2.10}$$

which does not exist because of the infinite product. Let us therefore look at the action on a local observable A. Note that the operations $A \mapsto U_x^* A U_x$ commute for different x because of Eq. (2.9), and that this action is the identity if $x+\mathcal{L}$ does not intersect the localization region of A. In the infinite product of these transformations only finitely many of them are different from the identity, and therefore the product defines an automorphism on local observables. Since according to the definition of the quasi-local algebra local observables are norm-dense, the automorphism can be extended to the whole algebra, i.e., we have that the limit

$$T(A) = \lim_{\Lambda \nearrow \mathbb{Z}^s} U_\Lambda^* A U_\Lambda \tag{2.11}$$

exists for all $A \in \mathcal{A}(\mathbb{Z}^s)$, where $U_\Lambda = \prod_{x \in \Lambda} U_x$ for a finite set Λ.

Note that the neighborhood scheme of the QCA is given by the union of all localization regions of the U_x, which intersect with $\{0\}$. Therefore, we have

$$\mathcal{N} = \mathcal{L} - \mathcal{L}\,. \tag{2.12}$$

The special case of single cell operations arises for $\mathcal{L} = \mathcal{N} = \{0\}$. More complicated examples occur by considering operators, which are diagonal in some product basis. In this case the QCA can be described by some local phases, but nevertheless allows interaction between different sites. A well-known example is an Ising interaction

$$H_x = Z_x \otimes Z_{x+1}\,, \tag{2.13}$$

where Z_x denotes the Pauli Z operator at position x. This interaction turned on for a finite time gives unitary operators U_x, which commute for different x. For a suitable time and followed by a single site operation, this interaction generates the cluster state, which is used as the initial entangled state of a one-way quantum computer, out of a product state [RB02].

Remarkably, a QCA defined by commuting unitaries shows no propagation, meaning that the localization region does not increase while iterating the QCA. This is simply because n steps of a QCA defined by U_0 are equivalent to a single time step of the QCA defined by U_0^n. Nevertheless, propagation can occur if we alternate between different QCAs defined by commuting unitaries, e.g., when we iterate the “cluster state generator”.

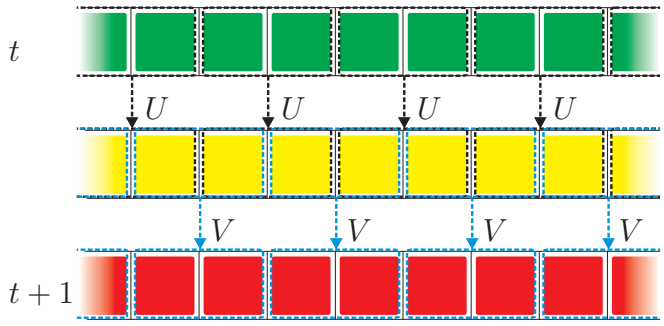

Figure 2.5: *A 1D QCA time step in Margolus partitioning form. The time step is decomposed into blockwise unitary transformations leading to an intermediate step.*

- **Margolus partitioning scheme:** For a QCA defined by commuting unitaries $U_x \in \mathcal{A}(\mathcal{L} + x)$, the applications of the unitaries can be organized in different layers, where in each layer only unitaries, which do not have overlapping localizations (i.e. $\mathcal{L} + x \cap \mathcal{L} + y = \emptyset$), are applied in parallel. The number of the required layers then clearly depends on the size of the localization region $\mathcal{L}$. A slight generalization of this scheme is given by using different unitaries for each layer, leading to a partitioning scheme established by Margolus in the classical case [Mar84]. In the simplest example, we have two layers of unitaries, where each unitary describes an interaction of two cells (see Figure 2.5).

- **Quantization of classical reversible cellular automata:** This method is described in detail in [SW04] and is only mentioned for completeness. Basically, the classical transition function allows to compute the matrix elements of the local rule of the QCA. One might think that the inverse neighborhood of the QCA, i.e. Eq. (2.8), contradicts the result of Kari that there is no upper bound on the neighborhood scheme of the inverse classical cellular automaton [Kar90], but the neighborhood of the QCA depends on the neighborhood of both the direct and the inverse cellular automaton.

- **Clifford quantum cellular automata:** These are QCAs, which map tensor products of Pauli operators to tensor products of Pauli operators. Therefore, the structure of these mappings can be described by classical rules with certain properties. These will be analyzed in detail in Chapter 4.

Clearly, each of these construction methods describes a subset of all reversible QCAs as defined in Definition 2.7. Now it would be nice to know whether some of these construction schemes suffice to generate all reversible QCAs. This would

show the equivalence of the axiomatic approach from above, which defines QCAs by basic principals, and a suitable constructive approach, which defines QCAs by a set of basic operations from which all QCAs can be achieved. Of course, it is possible that different combinations of construction methods are doing this job. For instance, as presented by the following result, all QCAs are obtained by a commuting unitaries scheme when we allow for an additional ancillary system. In contrast to this, we will show in Chapter 3 that conditional shifts and Margolus partitioning describe a sufficient set of operations, at least in one lattice dimension.

The implementation scheme of Arrighi et al. [ANW08] needs an additional ancillary system, i.e., the single cell algebra of the system is given by $\tilde{\mathcal{A}}_x = \mathcal{A}_x \otimes \mathcal{A}_x$. By rearranging the tensor factors the total system can thus be identified with $\tilde{\mathcal{A}}(\mathbb{Z}^s) = \mathcal{A}(\mathbb{Z}^s) \otimes \mathcal{A}(\mathbb{Z}^s)$.

Theorem 2.10 (Structure Theorem [ANW08]) *Let T be a QCA on $\mathcal{A}(\mathbb{Z}^s)$ and let $\mathbb{F}_x$ denote the Flip operation on the system $\tilde{\mathcal{A}}_x$. Then the operators*

$$U_x = (\mathrm{id}_{\mathcal{A}(\mathbb{Z}^s)} \otimes T)(\mathbb{F}_x) \tag{2.14}$$

are local unitaries on $\tilde{\mathcal{A}}(\mathbb{Z}^s)$ and commute. Hence, their product defines a QCA $\tilde{T}$ on $\tilde{\mathcal{A}}(\mathbb{Z}^s)$. This QCA fulfills

$$\begin{aligned} \tilde{T}(A \otimes \mathbb{1}) &= \mathbb{1} \otimes T(A)\,, & (2.15)\\ \tilde{T}(\mathbb{1} \otimes A) &= T^{-1}(A) \otimes \mathbb{1}\,. & (2.16) \end{aligned}$$

Proof: Since the $\mathbb{F}_x$ are unitary operators, which commute for $x \neq y$, after applying the automorphism $\mathrm{id}_{\mathcal{A}(\mathbb{Z}^s)} \otimes T$ they are still commuting unitaries, which are localized on $\tilde{\mathcal{A}}(\mathcal{N} + x)$ when $\mathcal{N}$ is the neighborhood scheme of T.

Now for $A_x \in \mathcal{A}_x$ we have

$$\begin{aligned} U_x^*(A_x \otimes \mathbb{1})U_x &= (\mathrm{id} \otimes T)(\mathbb{F}_x)(A_x \otimes \mathbb{1})(\mathrm{id} \otimes T)(\mathbb{F}_x)\\ &= (\mathrm{id} \otimes T)(\mathbb{F}_x(A_x \otimes \mathbb{1})\mathbb{F}_x)\\ &= (\mathrm{id} \otimes T)(\mathbb{1} \otimes A_x) = \mathbb{1} \otimes T(A_x)\,. \end{aligned}$$

Similarly, we have for $A_y \in \mathcal{A}_y$ $(y \neq x)$ that $U_x^*(A_y \otimes \mathbb{1})U_x = A_y \otimes \mathbb{1}$ holds because A_y and $\mathbb{F}_x$ commute. Hence, for the product of the U_x we have $A \otimes \mathbb{1} \mapsto \mathbb{1} \otimes T(A)$.

Analogously, we compute

$$\begin{aligned} U_x^*(\mathbb{1} \otimes A_x)U_x &= (\mathrm{id} \otimes T)(\mathbb{F}_x(\mathbb{1} \otimes T^{-1}(A_x))\mathbb{F}_x)\\ &= T^{-1}(A_x) \otimes \mathbb{1}\,, \end{aligned}$$

which proofs the rest of the theorem. ■

Basically, the Theorem tells us that the commuting unitaries defined by Eq. (2.14), followed by a Flip operation between the original system and the ancillary system, implement the QCA itself on one system and its inverse on the ancillary system. We will see in Chapter 3 that this additional system is in general indeed necessary when we insist on a local unitary scheme, and that the inverse automaton arises for "symmetrizing the information flow" in the total system. Alternatively, we will also find a scheme which allows an implementation by conditional shifts and Margolus partitioning, at least in one lattice dimension. Remarkably, both schemes also work without translation invariance (it is easy to see that translation invariance is not required for the foregoing proof).

2.3 Quantum Walks

A (classical) random walk describes a particle on some lattice, which moves in discrete time steps from one lattice position with certain probabilities to the neighboring lattice positions. A familiar example is a one-dimensional lattice $\mathbb{Z}$, where in each single time step a coin is thrown for deciding, whether the particle moves one position to the right or to the left, respectively. Thus, for an ideal fair coin the probability for going right or going left is each given by 1/2. But using different lattices and varying the probabilities allows versatile constructions of random walk processes, which can, for instance, be applied to search problems or diffusion processes.

Let us have a closer look at the standard example, i.e. a particle on $\mathbb{Z}$ with fair coin toss. Starting with the particle at the origin, we like to study the probability distribution in dependence of the number of time steps. Clearly, after an even number of time steps only even positions can be occupied, and the same is true when replacing even by odd. Now suppose after t time steps the particle has moved k times to the right and therefore $t-k$ to the left. Then its position is $2k-t$ and the probability can be computed by counting the number of possible paths, leading to

$$P(n = 2k - t) = \binom{t}{k} 2^{-t}. \tag{2.17}$$

This is a binomial distribution with expectation value 0 and variance t [Ros62], i.e. the expected translation distance after t time steps scales as $\sqrt{t}$. In the limit of small lattice constant and many time steps the probability distribution becomes a Gaussian distribution, which is in correspondence to the random walk evolution becoming equivalent to the diffusion equation [Ros62, Fel57].

A quantum version of such a random walk was first introduced in [ADZ93], where the outcome of a measurement of the z-component of a spin-1/2-particle determines, whether the particle moves right or left. Later, the measurement was replaced by a unitary rotation of the internal degree of freedom ("coin toss"), which allows fully coherent dynamics when iterating the quantum walk. To our

knowledge, such a model was first discussed by Meyer [Mey96a, Mey96b]. Note however that he uses the notation quantum cellular automata for this kind of model, in contrast to recent denotations. Formally, quantum walks have been introduced in [ABN$^+$01, NV00] on the line and in [AAKV01] on general graphs. A nice review is [Kem03], where all common models are described including continuous time quantum walks, which have been introduced by Farhi and Gutmann [FG98]. This continuous time model is not further discussed here because we focus on the discrete time case.

Here we like to describe the basic formalism of quantum walks ("QWs") on a lattice $\mathbb{Z}^s$. As already observed by Meyer, non-trivial unitary walks are only possible when we allow for an internal degree of freedom of the particle [Mey96b] (a simple proof of this statement can also be found in Chapter 6). The underlying Hilbert space thus decomposes into a tensor product $\mathcal{H} = \ell^2(\mathbb{Z}^s) \otimes \mathbb{C}^d$, where $\ell^2(\mathbb{Z}^s)$ describes the position space and $\mathbb{C}^d$ the internal states of the particle. Hence, the wave function of a particle assigns a vector $\psi(\vec{x}) = (\psi(\vec{x}, 1), \ldots, \psi(\vec{x}, d))^T \in \mathbb{C}^d$ to each lattice point, and the normalization condition is given by

$$\sum_{\vec{x}} \|\psi(\vec{x})\|^2 = \sum_{\vec{x}} \sum_{\alpha=1}^{n} |\psi(\vec{x}, \alpha)|^2 = 1\,. \tag{2.18}$$

The QW itself is now decomposed into a unitary coin toss C on the internal degree of freedom and a shift operation S which translates the basis vectors, where the translation vector $\vec{x}(\alpha)$ depends on the internal state. Therefore, this is called a conditional shift operation (see also the corresponding operations for QCAs from the previous Section). The QW is thus given by $U = (\mathbb{1} \otimes C)S$ and acts on a wave function as

$$(U\psi)(\vec{y}, \alpha) = \sum_{\beta=1}^{d} C_{\alpha\beta} \psi(\vec{y} - \vec{x}(\alpha), \beta)\,. \tag{2.19}$$

It is easy to see that a QW commutes with the shift operations $\psi(\vec{y}) \mapsto \psi(\vec{y} + \vec{x})$, i.e. a QW defined in this way is translationally invariant. Therefore, we like to use Fourier transform techniques to diagonalize the quantum walk in momentum space. We use

$$\hat{\psi}(\vec{p}) = \sum_{\vec{x}} \psi(\vec{x})\, e^{i\vec{p}\cdot\vec{x}} \tag{2.20}$$

as Fourier transform and

$$\psi(\vec{x}) = \frac{1}{(2\pi)^s} \int_{-\pi}^{\pi} \ldots \int_{-\pi}^{\pi} d\vec{p}\; \hat{\psi}(\vec{p})\, e^{-i\vec{p}\cdot\vec{x}} \tag{2.21}$$

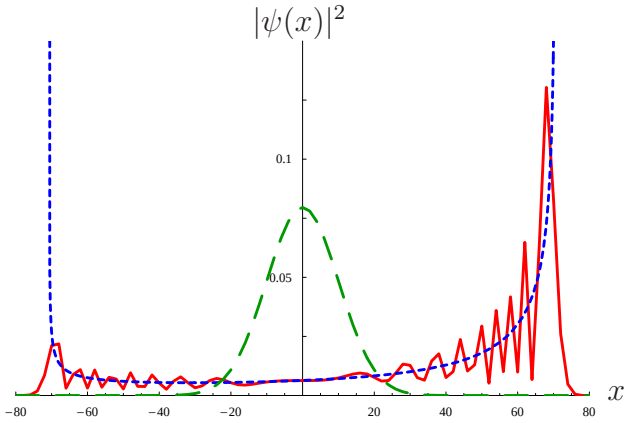

Figure 2.6: *Probability distribution of a random walk (green dashed line) compared to a quantum walk (red through line) after 100 time steps. The quantum walk is a Hadamard walk with initial state* $\psi_{in}(x) = (1,0)^T \delta_{x0}$. *This state leads to the velocity distribution in Eq. (2.31), which is also plotted in a suitable scaling (blue dotted line). Note that for both distributions only the probabilities on even positions are plotted.*

as inverse Fourier transform. The Fourier transform of the walk then yields

$$\hat{U}(\vec{p}) = \begin{pmatrix} e^{i\vec{p}\cdot\vec{x}(1)} & & 0 \\ & \ddots & \\ 0 & & e^{i\vec{p}\cdot\vec{x}(d)} \end{pmatrix} C\,. \tag{2.22}$$

For every $\vec{p}$ this matrix is unitary and can therefore be diagonalized, which leads to the spectral decomposition

$$\hat{U}(\vec{p}) = \sum_{\alpha=1}^{d} e^{i\omega_\alpha(\vec{p})} P_\alpha(\vec{p}) \tag{2.23}$$

with eigenvalues $e^{i\omega_\alpha(\vec{p})}$ and eigenprojectors $P_\alpha(\vec{p}) = |\,\hat{\psi}_\alpha(\vec{p})\rangle\langle\hat{\psi}_\alpha(\vec{p})|$.

Given any initial state, the iteration of the QW can be computed rather easily in momentum space, and inverse Fourier transform of the output state gives the probability distribution of the particle in position space. One generically finds that the probability distribution behaves very different in contrast to the classical case. Usually, the probability is very low around the origin and very high at the boundaries of the distribution. This leads to two peaks, which travel with a constant velocity. In particular, the spread out is proportional to the time, i.e. the QW propagates ballistically, whereas the random walk shows diffusive behavior (see Figure 2.6).

There have been several attempts to understand this behavior in detail, e.g. by calculating the asymptotic position distribution. For specific examples of

quantum walks this was already done in [NV00] by a stationary phase method and in [CIR03] via Jacobi polynomials, which arise in the path-integral representation of quantum walks. Nevertheless, these methods rely on very specific QWs and specific initial states. A more elegant and general way has been introduced by Grimmett, Janson and Scudo [GJS04b, GJS04a] by looking at weak limits of the position operator (see also the related work by Konno [KNS04, Kon05] and [Gat05] for the version presented here).

Theorem 2.11 ([GJS04b, Gat05]) *Let $Q_j = -i\frac{d}{dp_j}$ be the j-th component of the position operator and $Q_j(t) = \hat{U}^{-t} Q_j \hat{U}^t$ the position operator at time t. Then the scaled position operator converges weakly[2] towards a group velocity operator, i.e.*

$$w - \lim_{t\to\infty} \frac{Q_j(t)}{t} = V_j \,. \tag{2.24}$$

For a quantum walk of the form (2.23) the velocity operator is given by

$$V_j(\vec{p}) = \sum_{\alpha=1}^{d} \frac{\partial \omega_\alpha(\vec{p})}{\partial p_j} P_\alpha(\vec{p}) \,. \tag{2.25}$$

In particular, this Theorem proofs that the spread out of the QW propagates ballistically, similar to a free quantum particle on the line. The ω_j play thus the role of dispersion relations. Further analogies between a QW and a free particle can be established by using a QW with a specified coin as free dynamics and a locally modified coin as potential. With the help of scattering theory reflection and transmission coefficients of such a potential can be calculated and also bound states can occur [FH04a, FH04b, Gat05, FH07]. The main difference is that there is no energy scale since we only have a time evolution and not a Hamiltonian at hand. Therefore, there is no analogue of a ground state.

The asymptotic probability distribution of the QW is according to Eq. (2.24) determined by the velocity distribution of the initial state, i.e. by a function ρ such that

$$\langle \psi_{in} | f(V) |\, \psi_{in} \rangle = \int_{v_{min}}^{v_{max}} dv \rho(v) f(v) \tag{2.26}$$

holds for all continuous functions f.

Example 2.12 A frequently used QW is the Hadamard walk. We have two internal states ($d = 2$) and the coin is given by the Hadamard matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} . \tag{2.27}$$

[2]More precisely, in the strong resolvent sense meaning that $\mathrm{tr}(\rho f(A_n)) \to \mathrm{tr}(\rho f(A))$ for any density operator ρ and continuous function f on $\mathbb{R}$ vanishing at infinity.

The conditional shift is in momentum space given by

$$S(p) = \begin{pmatrix} e^{ip} & \\ & e^{-ip} \end{pmatrix} . \tag{2.28}$$

The basis vectors are therefore often denoted by $|\, R\rangle$ ("go right") and $|\, L\rangle$ ("go left"). The eigenvalues in momentum space are $e^{i\omega_+(p)} = e^{i\omega(p)}$ and $e^{i\omega_-(p)} = e^{i(\omega(p)+\pi)}$ with the dispersion relation

$$\sin\omega = \frac{\sin p}{\sqrt{2}} . \tag{2.29}$$

The group velocity operator is according to Eq. (2.25) given by

$$V(p) = \frac{\cos p}{1+(\cos p)^2} \begin{pmatrix} \cos p & e^{-ip} \\ e^{ip} & -\cos p \end{pmatrix} , \tag{2.30}$$

which leads for the initial state $\psi_{in}(x) = (1,0)^T \delta_{x0}$ to the velocity distribution

$$\rho(v) = \left(\pi(1-v)\sqrt{1-2v^2}\right)^{-1} . \tag{2.31}$$

The probability distribution after 100 time steps and the velocity distribution are depicted in Figure 2.6. ◊

Part I

Quantum Cellular Automata

Chapter 3

Index Theory of Quantum Cellular Automata

In this Chapter we introduce the index of a one-dimensional quantum cellular automaton by the normalized information flow to the right, or to the left respectively. By construction, this is a positive rational number and locally computable. But even without translation invariance, the index is constant along the line, i.e. a global quantity. We show that the index is multiplicative under compositions of quantum cellular automata, both for successive execution as for composition of independent parallel systems. Furthermore, we find that the index quantifies the amount of ancillary space needed for a local implementation scheme. In particular, quantum cellular automata with trivial index can be implemented by a circuit of local unitaries without any ancilla space. We show that this is also exactly the subclass of quantum cellular automata which can be locally deformed to the identity and which can be decoupled by a local operation to independent dynamics on the half-chains.

3.1 Introduction

For the study of the general structure of quantum cellular automata the index theory turns out to be a very versatile and important tool, i.e., the index helps to answer many important questions in the general theory of reversible quantum cellular automata. These will be described in the following paragraphs.

3.1.1 Physical Motivation

We have seen in Theorem 2.10 (adapted from [ANW08]) that all QCAs can be implemented by a circuit of local unitaries if we allow for an additional ancillary system. On the other hand, it is also possible to construct QCAs which do not need such an ancillary system for a local implementation, e.g. a QCA defined by

commuting unitaries. Given any arbitrary QCA, this gives rise to the question, whether we need an ancillary system for a local implementation scheme, or how much of this system is essentially used by the local unitary circuit. Of course, it should be possible to answer this question efficiently, e.g. by local data. We will present a way to compute the required ancilla space from the local rule of the automaton.

In the experimental setup, e.g. in optical lattices, the control of global parameters is often easily possible, whereas the control of local parameters is a hard task. So it would be nice to know, how global parameters can limit the possibilities for the local dynamics, i.e. which local rules can be tuned continously into each other without changing the global parameters (*local equivalence*). This is also an interesting question when one wants to study the connection to continuous time evolutions, in particular, for the mutual simulatability of continuous and discrete time evolution. Since a continuous time evolution can always be continuously deformed to the identity, this should also be true for the corresponding discrete time evolution.

We do not assume translation invariance in this Chapter, so we allow for different local rules for each single cell. Since neighboring local rules must obey some commutation relations (compare Lemma 2.8), it is clear that not all valid local rules can be combined, i.e., not all of them can be executed in parallel. Now the interesting question is to decide which local rules can and which cannot be combined. Especially, it would be nice to have some quantity which distinguishes between different classes of local rules, i.e. which is constant for all combinable local rules and different for local rules which cannot be combined.

Another important task is to look for the information flow in a quantum cellular automaton. It is clear that, in general, it is possible to send information from left to right or from right to left, although only with a bounded velocity. But there are also QCAs, e.g. a shift, where information can only be send in one direction. So it would be nice to characterize the *mean information flow* from the local rule of the automaton, i.e. the ratio of information send to the right and to the left, respectively. Furthermore, for the non-translationally invariant case it would be nice to know, if or how much the mean information flow can differ throughout the lattice.

3.1.2 Mathematical Motivation

Although we have addressed quite a variety of physically interesting problems, the mathematical problem is quite intuitive. Let us fix for a moment the observable algebra, i.e. all single cell dimensions. Then the set of all QCAs, i.e. all local automorphisms on this algebra, defines a group with respect to multiplication. Now the task is to characterize the connected components of this group, i.e. to classify which QCAs can be continously deformed into each other within the group of QCAs. Furthermore, we have to define a quantity (the *index* of a

QCA) which distinguishes between these connected components and which can be computed efficiently for each QCA, i.e. by local data. Although this is, to some extend, a basic task in group theory[1], the mathematical details of this problem crucially depend on the structure of the group and cannot be simply adapted from corresponding problems for other groups, e.g., we will see in Chapter 7 that the mathematical tools are very different in the case of quantum walks. Another problem is to handle QCAs on different cell structures, i.e. on different observable algebras.

We will present both an axiomatic characterization, as well a constructive definition of the index, i.e., we show how to compute the index for any given QCA and we know that this is essentially the only quantity which comes into consideration for the classification of locally equivalent QCAs.

3.1.3 Index Theory of Classical Reversible Cellular Automata

We would like to mention that there is also an index quantity defined in the case of classical reversible cellular automata (see e.g. [Hed69, CK05]) called the "Welch index" of a cellular automaton. Given some configuration c on all cells $x > 0$, consider the number of possible states in the cell $x = 0$, such that after one time step the configuration on the right hand side is (by a suitable choice of states on cells $x > 0$ before the time step) equal to c. It can be shown that this number of states is independent of the chosen configuration and it is called the *left Welch index*. Of course, the *right Welch index* can be defined in the corresponding way.

Nevertheless, the index theory we would like to establish for quantum cellular automata corresponds more to a construction by Jarkko Kari [Kar96, Kar05a] although he does not use the name "index". For a given configuration on the whole lattice he constructs a subtle combination of a block of this configuration with a block of its image under the cellular automaton, where the block of the image is translated to the right, or to the left respectively, from the configuration block. By running through all possible configurations this gives two finite sets which correspond to our information flows defined in Definition 3.2. The cardinality of one of the sets, normalized by the cell dimension, then corresponds to our index quantity. This gives, analogous to our construction, a homomorphism from the group of reversible cellular automata to the group of positive rationals. Furthermore, the indices of block permutations, or respectively blockwise unitary transformations, and shift operations are in one-to-one correspondence to our case.

[1] A prominent example is the group $O(n)$, i.e. all orthogonal transformations in $\mathbb{R}^n$, where the connected components are distinguished by the determinant $\det : O(n) \to \{-1, 1\}$.

3.1.4 Quantum Cellular Automata without Translation Symmetry

First we have to modify the definition of one-dimensional quantum cellular automata to the non translation invariant case. We do not only allow the local rules to be different for each lattice site, but also for inhomogeneous cell dimensions. The observable algebra at position $x \in \mathbb{Z}$ is denoted by $\mathcal{A}_x \cong \mathcal{M}_{d(x)}$, i.e. isomorphic to the algebra of $d(x) \times d(x)$-matrices. The infinite tensor product of these algebras is defined in the sense of quasi-local algebras (see Subsection 2.1.2). This algebra will be denoted by $\{\mathcal{A}_x\}_{x\in\mathbb{Z}}$ and also referred to as cell structure.

Since we drop translation invariance, the definition of a QCA on such a system reduces to a local automorphism[2] T, i.e., there exists $N \in \mathbb{N}$ (the neighborhood or *width* of the QCA) such that for all $x \in \mathbb{Z}$ the image of $\mathcal{A}_x$ under T is contained in $\mathcal{A}([x - N, x + N])$. A slight generalization of Lemma 2.8 then shows that the homomorphisms $T_x := T|_{\mathcal{A}_x}$ uniquely determine T and that the algebras $T_x(\mathcal{A}_x)$ for different x have to commute elementwise. In this case these homomorphisms are referred to as local rules.

Note that it is possible to group cells together and to redefine the action of the QCA such that we have only nearest neighbor interactions, i.e., we can set $N = 1$ for convenience. Since the dimensions of the grouped cells are multiplied to the "new" single cell dimension, the cells might get very large in some cases.

3.1.5 Outline and Summary of Results

In Section 3.2 we first give some axioms which should be fulfilled by the index quantity. Afterwards we define the information flows in the dynamics of a QCA and show that there is some ratio which is constant along the line, even without assuming translation invariance. This behavior suggests to identify this ratio with the index, and by studying the fundamental properties of this quantity in Section 3.3 we find that all our axioms are fulfilled. For instance, we find that the index is multiplicative under tensor products and compositions of QCAs, and that the only QCAs, which can be locally decoupled into independent dynamics on the half-chains and which can be locally deformed to the identity, are exactly those with trivial index. Furthermore, it also turns out that this is the subgroup of QCAs, which can be locally implemented without any ancillary space.

In Section 3.4 we consider QCAs in higher lattice dimensions. Similar results are only expected to hold with translation invariance, but even with this restriction we are only able to make a detailed analysis for special neighborhood schemes. All these examples hint that there is some corresponding index quantity in higher dimensions, but for the general case we have not been able to define it in a satisfactory way.

[2]We replace homomorphism by automorphism, since without translation invariance the reversibility does not follow from the Wrapping Lemma 2.9.

3.2 Basic Definitions

In this Section we will both characterize the index in an axiomatic approach as well as define the index by local data of the automorphism. Readers, who are not interested in the axiomatic characterization, can just switch to the constructive approach (Subsection 3.2.2).

3.2.1 Axiomatic Characterization

We would like to establish an axiomatic characterization of the index $\operatorname{ind} T$ of a quantum cellular automaton T, i.e., we have to give some requirements which should be satisfied by the index and these requirements have to determine the index function. The only requirements which should be satisfied in this case are the following: It should be possible to compute the index from local data, i.e., by the action of T on a local algebra $\mathcal{A}(\Lambda)$ where Λ is of the order of the neighborhood of T. We also demand that the index does not depend on where this finite region is localized on the chain. This means we look for a locally computable quantity which is constant along the chain, i.e. of global relevance, although no translation invariance is assumed.

Quantum cellular automata with the same index are assumed to be *locally equivalent* which is formally phrased in the following equivalence relation.

Definition 3.1 *Let T and T' be quantum cellular automata on possibly different quasi-local algebras $\{\mathcal{A}_x\}_{x\in\mathbb{Z}}$ and $\{\mathcal{A}'_x\}_{x\in\mathbb{Z}}$, both with neighborhood scheme $\mathcal{N} \subset \mathcal{N}_N := [-N, N]$. We say that T and T'* **share an interval** *$I \subset \mathbb{Z}$ if $|I| \geq N$, and there are isomorphisms $j_x : \mathcal{A}_x \to \mathcal{A}'_x$ for all $x \in I + \mathcal{N}_N$ such that with $j = \bigotimes_{x\in I+\mathcal{N}_N} j_x$ we have $T'j(A) = j\,T(A)$ for all $A \in \mathcal{A}(I)$.*

We denote $T \sim T'$, if T and T' can be linked by a chain of QCAs such that any two neighbors on this chain share an interval. The class of T under this equivalence relation is defined by $[T]$.

This equivalence relation features some basic properties:

- *Crossover:* If T and T' share an interval $I = [a, b]$, we can construct a third automaton T'' which complies with T on the left hand side of the chain and with T' on the right hand side of the chain (*crossover*). We simply have to take the cell structure and the local rules of T for all $x < a$ and of T' for all $x > b$. On the interval I it does not matter which rules we use as long as we account for the appropriate isomorphisms. The existence of such a crossover is a convenient condition to verify $T \sim T'$ since we do not need any assumptions about some cells of the automata being isomorphic.

- *Decoupled quantum cellular automata:* We say a QCA T is *decoupled* if the subalgebras $\mathcal{A}_L = \mathcal{A}(\{x|\, x \leq 0\})$ and $\mathcal{A}_R = \mathcal{A}(\mathbb{N})$ are invariant, i.e. the

QCA decomposes into a tensor product $T = T_L \otimes T_R$. Now suppose we have two decoupled QCAs T and T' (on possibly different cell structures), then $T_L \otimes T'_R$ (or $T'_L \otimes T_R$ alternatively) is a crossover between T and T', i.e. these are in the same equivalence class. In particular, the identity on any cell structure is trivially decoupled, i.e. the class [id] contains all decoupled QCAs.

- *Tensor products:* If T and T' are QCAs, their tensor product $T \otimes T'$ is defined by taking the tensor product of the local rules on the cell structure $\{\mathcal{A}_x \otimes \mathcal{A}'_x\}_{x\in\mathbb{Z}}$, i.e., here the tensor product describes a split in the local cell space and not, as compared to the last paragraph, in position space. Clearly, the tensor product is compatible with the equivalence relation, i.e., if $T \sim S$ and $T' \sim S'$ we also have $T \otimes T' \sim S \otimes S'$. Since also $T \otimes T' \sim T' \otimes T$ holds, we can define a commutative and associative composition on the equivalence classes by
$$[T][T'] = [T \otimes T']\,. \tag{3.1}$$
In particular, the class [id] is the identity for this composition.

- *Group structure:* Let T and T' be QCAs on the same cell structure, such that it is possible to multiply them. The cell structure of $T \otimes T'$ has then two factors $\mathcal{A}_x$ for every x. Let S denote the automorphism, which exchanges these copies for every $x \geq 0$, but does nothing for $x < 0$. Then we have
$$\begin{aligned} T \otimes T' &= (T \otimes \mathrm{id})(\mathrm{id} \otimes T') \sim (T \otimes \mathrm{id})S(\mathrm{id} \otimes T')S \\ &\sim (T \otimes \mathrm{id})(T' \otimes \mathrm{id}) = T \circ T' \otimes \mathrm{id} \sim T \circ T'\,. \end{aligned}$$
For the first equivalence the QCAs coincide for all $x < -N$, for the second equivalence for all $x > N$ and the last one follows because, according to the previous paragraph, tensoring with the identity does not change the equivalence class. So we also have $[T \circ T'] = [T][T']$ and, since the inverse of a QCA is again a QCA, for every class there exists an inverse element, i.e. the classes $[T]$ form an abelian group, the *abstract index group*.

- *Shift operations:* Let us consider the right shift τ_d on the cell structure with $\mathcal{A}_x \equiv \mathcal{M}_d$. For a composite number $d = d_1 d_2$ the shift decomposes into $\tau_d = \tau_{d_1} \otimes \tau_{d_2}$, i.e., by the product formula, we only need to know the equivalence classes of the prime number shifts: for $d = \prod_i p_i^{n_i}$ we have $[\tau_d] = \prod_i [\tau_{p_i}]^{n_i}$. When we consider a composition of right and left shift, e.g. $\tau_n \otimes \tau_m^{-1}$, we see that the class only depends on n/m. In particular, factors of the type $\tau_d \otimes \tau_d^{-1}$ cancel.

This gives rise to the conjecture that the abstract index group is isomorphic to the multiplicative group of positive rational numbers, and that the index of a composed shift $\tau_n \otimes \tau_m^{-1}$ can be identified with n/m. This would have many important

consequences, e.g. all compositions of shifts would be sufficient for representing all equivalence classes, and no crossover between shifts of relatively prime dimensions could exist. In the next Subsection we will show by a constructive definition that this is indeed correct.

3.2.2 Constructive Approach

We try to quantify the information flow in a one-dimensional quantum cellular automaton. The cell structure is given by $\{\mathcal{A}_x\}_{x\in\mathbb{Z}}$ with $\mathcal{A}_x = \mathcal{M}_{d(x)}$, and, if necessary, by regrouping of the cells, we may assume that $N = 1$ holds, i.e., we consider a QCA with nearest neighbor interaction. An important tool will be the concept of *support algebras*, which is described in Appendix A.

We want to study the information flow of the QCA, i.e. the ratio of information send to the right and to the left, respectively. Since the QCA acts locally, we can locally look for the information flow. Therefore we consider the image of two neighboring cells $\mathcal{A}_{2x} \otimes \mathcal{A}_{2x+1}$ for $x \in \mathbb{Z}$. We have

$$T(\mathcal{A}_{2x} \otimes \mathcal{A}_{2x+1}) \subset (\mathcal{A}_{2x-1} \otimes \mathcal{A}_{2x}) \otimes (\mathcal{A}_{2x+1} \otimes \mathcal{A}_{2x+2})\,. \tag{3.2}$$

Of course, the brackets are not really relevant, but they are placed to divide the algebras on the left hand side from the algebras on the right hand side. In general, the algebras $\mathcal{A}_{2x-1}\otimes\mathcal{A}_{2x}$ and $\mathcal{A}_{2x+1}\otimes\mathcal{A}_{2x+2}$ are larger than what is really needed to describe the image of $\mathcal{A}_{2x}\otimes\mathcal{A}_{2x+1}$, i.e., there are subalgebras $\mathcal{L} \subset \mathcal{A}_{2x-1}\otimes\mathcal{A}_{2x}$ and $\mathcal{R} \subset \mathcal{A}_{2x+1}\otimes\mathcal{A}_{2x+2}$ such that $T(\mathcal{A}_{2x}\otimes\mathcal{A}_{2x+1})$ is still contained in the tensor product $\mathcal{L}\otimes\mathcal{R}$. The smallest possible of such subalgebras are exactly the ones given by the support algebras.

Definition 3.2 *The* **flow to the right** $\mathcal{R}_{2x}$ *of a QCA at position* $2x \in \mathbb{Z}$ *is defined by the support algebra of* $T(\mathcal{A}_{2x}\otimes\mathcal{A}_{2x+1})$ *in* $\mathcal{A}_{2x+1}\otimes\mathcal{A}_{2x+2}$*, i.e.*

$$\mathcal{R}_{2x} := S\left(T(\mathcal{A}_{2x}\otimes\mathcal{A}_{2x+1}), \mathcal{A}_{2x+1}\otimes\mathcal{A}_{2x+2}\right)\,. \tag{3.3}$$

Analogously, the **flow to the left** *is defined by*

$$\mathcal{L}_{2x} := S\left(T(\mathcal{A}_{2x}\otimes\mathcal{A}_{2x+1}), \mathcal{A}_{2x-1}\otimes\mathcal{A}_{2x}\right)\,. \tag{3.4}$$

Now, the only algebras which are localized in the cells $2x-1$ and $2x$ are $\mathcal{R}_{2(x-1)}$ and $\mathcal{L}_{2x}$, in particular all the other algebras automatically commute with these two. The structure of support algebras will allow us to show that $\mathcal{R}_{2(x-1)}$ and $\mathcal{L}_{2x}$ also commute, i.e., all the algebras $\mathcal{R}_{2x}$ and $\mathcal{L}_{2x}$ commute. We will also find that these are isomorphic to full matrix algebras, and this observation will be the starting point for the definition of the index.

Theorem 3.3 *For every* $x \in \mathbb{Z}$ *the algebras* $\mathcal{R}_{2x-2}$ *and* $\mathcal{L}_{2x}$ *commute and are isomorphic to full matrix algebras, i.e. there exist real numbers* $r(2x-2)$ *and* $l(2x)$ *with*

$$\mathcal{R}_{2x-2} \cong \mathcal{M}_{r(2x-2)} \quad \textit{and} \quad \mathcal{L}_{2x} \cong \mathcal{M}_{l(2x)}\,. \tag{3.5}$$

Proof: The algebras are given by

$$\begin{aligned} \mathcal{R}_{2x-2} &= S\left(T(\mathcal{A}_{2x-2}\otimes\mathcal{A}_{2x-1}), \mathcal{A}_{2x-1}\otimes\mathcal{A}_{2x}\right) \\ \mathcal{L}_{2x} &= S\left(T(\mathcal{A}_{2x}\otimes\mathcal{A}_{2x+1}), \mathcal{A}_{2x-1}\otimes\mathcal{A}_{2x}\right) . \end{aligned}$$

In particular, since T is an automorphism, the images of the algebras $\mathcal{A}_{2x}\otimes\mathcal{A}_{2x+1}$ and $\mathcal{A}_{2x-2}\otimes\mathcal{A}_{2x-1}$ commute, and, because the whole overlap of these images is contained in $\mathcal{A}_{2x-1}\otimes\mathcal{A}_{2x}$, the support algebras also commute according to Lemma A.1.

Suppose that any $\mathcal{R}_{2x}$ (or $\mathcal{L}_{2x}$, respectively) has a non-trivial center, i.e., there exists one element $A \notin \mathbb{C}\mathbb{1}$ which commutes with all operators in $\mathcal{R}_{2x}$. In particular, this operator then commutes with all operators of the algebra, which is generated by all $\mathcal{R}_{2y}$ and $\mathcal{L}_{2y}$. Since this algebra contains by construction the image of the whole quasi-local algebra under T, A has to commute with $T(\mathcal{A}(\mathbb{Z})) = \mathcal{A}(\mathbb{Z})$, i.e. the whole quasi-local algebra, which has, contradictorily, a trivial center. ■

We have shown how to locally quantify the amount of information transfer to the right and to the left, respectively. But we are looking for a global quantity, i.e. a quantity which is constant along the whole chain. Therefore, we have to "normalize" with the single cell dimensions.

Theorem 3.4 *With $\mathcal{R}_{2x} \cong \mathcal{M}_{r(2x)}$, $\mathcal{L}_{2x} \cong \mathcal{M}_{l(2x)}$ and $\mathcal{A}_x = \mathcal{M}_{d(x)}$, the dimensions of the matrix algebras fulfill*

$$\frac{r(2x-2)}{d(2x-1)} = \frac{d(2x)}{l(2x)} = \frac{r(2x)}{d(2x+1)} . \tag{3.6}$$

Proof: The algebras $\mathcal{L}_{2x}$ and $\mathcal{R}_{2x-2}$ are contained in $\mathcal{A}_{2x-1}\otimes\mathcal{A}_{2x}$ and thereby its tensor product, too. Since $\mathcal{L}_{2x}$ and $\mathcal{R}_{2x-2}$ are the only support algebras, which are localized in $\mathcal{A}_{2x-1}\otimes\mathcal{A}_{2x}$, and the image of T must contain $\mathcal{A}_{2x-1}\otimes\mathcal{A}_{2x}$, we have $\mathcal{L}_{2x}\otimes\mathcal{R}_{2x-2} \cong \mathcal{A}_{2x-1}\otimes\mathcal{A}_{2x}$, i.e. $l(2x)r(2x-2) = d(2x-1)d(2x)$. On the other hand, $\mathcal{L}_{2x}\otimes\mathcal{R}_{2x}$ contains the image of $\mathcal{A}_{2x}\otimes\mathcal{A}_{2x+1}$, i.e.

$$T(\mathcal{A}_{2x}\otimes\mathcal{A}_{2x+1}) \subset \mathcal{L}_{2x}\otimes\mathcal{R}_{2x} .$$

This inclusion cannot be strict, since otherwise $\mathcal{L}_{2x}$, or $\mathcal{R}_{2x}$ respectively, would contain some element which commutes with the image of the whole quasi-local algebra under T. So we also have $l(2x)r(2x) = d(2x)d(2x+1)$. ■

Definition 3.5 *The* **index** *of a one dimensional QCA T on the cell structure $\{\mathcal{M}_{d(x)}\}_{x\in\mathbb{Z}}$ with $\mathcal{R}_{2x} \cong \mathcal{M}_{r(2x)}$ is defined by*

$$\mathrm{ind}(T) = \frac{r(2x)}{d(2x+1)}\,, \tag{3.7}$$

and, according to Theorem 3.4, independent of the lattice point x.

This definition connects the index with the information flow to the right. Of course, a similar definition can be based on the information flow to the left, but this would only replace the index with its reciprocal value. Also the even/odd asymmetry comes only from this special construction, and the results are not different when shifting the whole construction by one position. In any case we have found the index quantity, which is locally computable and constant along the chain.

3.2.3 Reduced Definition

We defined the index directly by looking at the entire cell structure, which is a bit against the philosophy that it is a locally computable quantity. We therefore simplify the definition, in such a way that it makes minimal use of the cell structure.

Consider any decomposition $\mathcal{A}(\mathbb{Z}) = \mathcal{A}_L \otimes \mathcal{A}_M \otimes \mathcal{A}_R$, where $\mathcal{A}_M \cong \mathcal{M}_d$ is contained in some local algebra $\mathcal{A}([x,y])$ with finite $x, y \in \mathbb{Z}$. We assume that $\mathcal{A}((-\infty, x-1]) \subset \mathcal{A}_L$ and $\mathcal{A}([y+1,\infty)) \subset \mathcal{A}_R$. Thus $\mathcal{A}_M$ may be a cell, or the local algebra of a larger interval, but may also contain matrix subalgebras of some neighboring cells. In any case, we will consider it as a cell in a locally modified cell structure. The important assumption about this decomposition is only that $\mathcal{A}_M$ is not too small compared to the neighborhood of the QCA T whose index we want to determine: we assume that $T(\mathcal{A}_R) \subset \mathcal{A}_M \otimes \mathcal{A}_R$ and $T(\mathcal{A}_L) \subset \mathcal{A}_L \otimes \mathcal{A}_M$. Defining $\mathcal{R}_M = S(T(\mathcal{A}_L \otimes \mathcal{A}_M), \mathcal{A}_M \otimes \mathcal{A}_R)$, the arguments of the previous paragraphs show that $\mathcal{R}_M$ and $T(\mathcal{A}_R)$ commute and together span the algebra $\mathcal{A}_M \otimes \mathcal{A}_R$. Because of the finite neighborhood scheme, the overlap of $T(\mathcal{A}_L \otimes \mathcal{A}_M)$ in the algebra $\mathcal{A}_M \otimes \mathcal{A}_R$ is finite, in particular, the algebra $\mathcal{R}_M$ is finite dimensional and has, by corresponding arguments from above, trivial center. This means we have $\mathcal{R}_M \cong \mathcal{M}_r$ for some $1 \le r \le d^2$ and we then define

$$\mathrm{ind}(T) = \frac{r}{d}\,. \tag{3.8}$$

It is also possible to cut the algebras $\mathcal{A}_L$ and $\mathcal{A}_R$ at the outer sides, such that the tensor product $\mathcal{A}_L \otimes \mathcal{A}_M \otimes \mathcal{A}_R$ is a finite dimensional algebra. We only need that this algebra still contains the image of $\mathcal{A}_M$. This approach would not require the calculation of images of infinite dimensional algebras and corresponds more to the constructive definition without assuming nearest neighbor interactions.

Note that a cut into two blocks, e.g. $\tilde{\mathcal{A}}_L \otimes \tilde{\mathcal{A}}_R$, does not allow the computation of the index in this way. There are QCAs, e.g. Clifford QCAs, where the support algebra of $T(\tilde{\mathcal{A}}_L)$ in $\tilde{\mathcal{A}}_R$ is abelian and, in particular, not isomorphic to a full matrix algebra.

Nevertheless, there is a possibility to calculate the index by a two block split, which is due to David Gross. Therefore, we have to equip each single cell with the Hilbert-Schmidt scalar product $\mathrm{tr} A^* B/d_x$ for $A, B \in \mathcal{A}_x$. Now for a QCA T of width N, let P_L denote the Hilbert-Schmidt projection operator onto $\mathcal{A}_{x-N} \otimes \ldots \otimes \mathcal{A}_x$ and P_R the projection onto $\mathcal{A}_{x+1} \otimes \ldots \otimes \mathcal{A}_{x+N+1}$. Then the index can be calculated by

$$\mathrm{ind}\, T = \frac{\mathrm{Tr}(T\, P_L\, T^*\, P_R)}{\mathrm{Tr}(T\, P_R\, T^*\, P_L)}, \tag{3.9}$$

where Tr denotes the tracial state induced by the Hilbert-Schmidt scalar product. This formula is also close to the definition of the index in the case of quantum walks (see Section 7.2).

3.2.4 Connection to the Jones Index

We like to state the connection between the index theory of QCAs to the Jones index for subfactors of von Neumann algebras. This may help to generalize the index theory to approximately local automorphisms or even irreversible, but local transformations. Here we only describe briefly the connections and readers, who are not interested in that, can just skip this Subsection.

Basically, the Jones index describes the multiplicity of subfactors of type II_1 von Neumann algebras (see [Jon83] or Chapter 19 of [Tak03]). For a subfactor $\mathcal{X} \subset \mathcal{Y}$ the Jones index is denoted by $[\mathcal{Y} : \mathcal{X}]$. For type II_1 factors $\mathcal{X} \subset \mathcal{Y} \subset \mathcal{Z}$ the basic properties of the Jones index are $[\mathcal{Z} : \mathcal{X}] \geq [\mathcal{Z} : \mathcal{Y}] \geq 1$, the chain rule $[\mathcal{Z} : \mathcal{Y}][\mathcal{Y} : \mathcal{X}] = [\mathcal{Z} : \mathcal{X}]$, and $[\mathcal{Z} : U^* \mathcal{X} U] = [\mathcal{Z} : \mathcal{X}]$ for a unitary $U \in \mathcal{Z}$. Furthermore, for the finite factor $\mathcal{M}_d$ we have

$$[\mathcal{M}_d \otimes \mathcal{Z} : \mathbb{1} \otimes \mathcal{X}] = d^2 [\mathcal{Z} : \mathcal{X}]\,. \tag{3.10}$$

This implies that all numbers d^2 for $d \in \mathbb{N}$ are possible values of the index. However, as shown by Jones the range of the index is more complicated. We have $[\mathcal{Z} : \mathcal{X}] \in \{4\cos(\pi/n)^2 | n \geq 3\} \cup [0, \infty]$, i.e. a combination of discrete values and a continuous interval, and for each value in this set there is a subfactor of the hyperfinite II_1 factor with a corresponding index.

The connection to the index of QCAs is given by considering the image of any left half chain $\mathcal{A}_L$. Basically, the half chain algebras can be regarded as type II_1 factors (see [KMSW06] for details). As in the previous Subsection we find for any QCA T a finite algebra $\mathcal{A}_M$ such that $T(\mathcal{A}_L) \subset \mathcal{A}_L \otimes \mathcal{A}_M$ holds and the

indices are related by

$$\mathrm{ind}(T) = \sqrt{\frac{[\mathcal{A}_L \otimes \mathcal{A}_M : T(\mathcal{A}_L)]}{[\mathcal{A}_L \otimes \mathcal{A}_M : \mathcal{A}_L]}}\,. \tag{3.11}$$

However, in our case only the trivial values d^2 of the Jones index are important. In general, the Jones index handles more complicated situations and may therefore help to transfer our index theory to more general transformations.

3.3 Fundamental Properties

We have defined the index of a one dimensional QCA constructively in terms of the information flow in the dynamical system. In this Section we will show that this definition fulfils all the properties, which we have assumed in the axiomatic characterization. But first we will show that the index quantifies the amount of local work space, which is essentially needed for a local implementation scheme, i.e., we can give bounds on the dimensions of the local ancilla space and, by construction, it is clear that these bounds are strict.

Theorem 3.6 *A nearest neighbor QCA T on the cell structure $\{\mathcal{M}_{d(x)}\}_{x\in\mathbb{Z}}$ with index t can be implemented by a circuit of local unitaries on the cell structure $\{\mathcal{M}_{d'(x)}\}$ with $d'(2x) = \max(1/t, 1)d(2x)$ and $d'(2x+1) = \max(t, 1)d(2x+1)$.*

Proof: From the construction of the index we have that $\mathcal{L}_{2x} \otimes \mathcal{R}_{2x}$ is isomorphic to $\mathcal{A}_{2x} \otimes \mathcal{A}_{2x+1}$, and that $\mathcal{R}_{2x-2} \otimes \mathcal{L}_{2x}$ is isomorphic to $\mathcal{A}_{2x-1} \otimes \mathcal{A}_{2x}$, both for every $x \in \mathbb{Z}$. So the corresponding isomorphisms on the whole chain naturally decompose into blockwise unitary transformations, and together they implement the QCA transformation (see Figure 3.1), similar to a Margolus partitioning scheme, but with different cells in the intermediate step. But, these unitaries will in general connect different cell structures. To circumvent this, one only has to embed the algebras of the chain and the algebras in the intermediate step, i.e. $\mathcal{L}_{2x}$ and $\mathcal{R}_{2x}$, in a common cell structure $\{\mathcal{M}_{d'(x)}\}$. This means we must have $d'(2x) = \max(l(2x), d(2x)) = \max(1/t, 1)d(2x)$ and $d'(2x+1) = \max(r(2x), d(2x+1)) = \max(t, 1)d(2x+1)$. The action of the isomorphisms can then simply be extended to a unitary on the common cell structure. ■

In particular, a QCA T with trivial index, i.e. $\mathrm{ind}(T) = 1$, can be locally implemented without any ancillary system in a Margolus partitioning scheme (see Subsection 2.2.2). In the translation invariant case we have two layers of tensor products of equal unitaries, but we cannot guarantee that, compared to the general case, the unitaries in the two layers are equal, i.e., by construction the translation invariance of the implementation is broken and is only given under even translations.

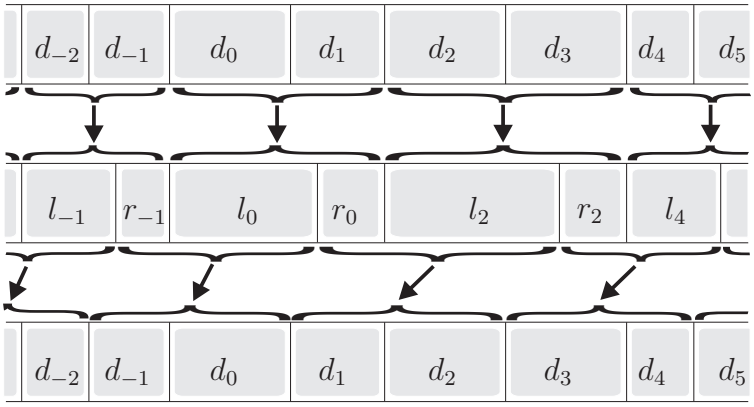

Figure 3.1: *Isomorphisms between cell structure and left/right flows (intermediate step), which break down into blockwise transformations. For a local unitary implementation the algebras have to be embedded into the same cell structure.*

Theorem 3.7

(*i*) $[T] \mapsto \mathrm{ind}(T)$ *is an isomorphism of the abstract index group described in Subsection 3.2.1 into the multiplicative group of positive rationals.*

(*ii*) *In particular,* $\mathrm{ind}(T \circ \tilde{T}) = \mathrm{ind}(T \otimes \tilde{T}) = \mathrm{ind}(T)\mathrm{ind}(\tilde{T})$, *and* $\mathrm{ind}(\tau_d) = d$.

(*iii*) *A QCA T admits a local decoupling, if and only if* $\mathrm{ind}(T) = 1$, *i.e., there exists an automorphism S, which acts like identity on all but finitely many cells, such that $S \circ T$ is decoupled.*

(*iv*) *Two QCAs T and $\tilde{T}$ on the same cell structure have the same index if and only if they can be locally deformed to each other, i.e., there is a norm continuous path $[0,1] \ni t \mapsto T_t$ of local automorphisms of uniformly bounded width such that $T_0 = T$ and $T_1 = \tilde{T}$.*

Proof:

(*i*) It is clear by construction that the index of a QCA is a positive rational. Further, we have $\mathrm{ind}(\mathrm{id}) = 1$, i.e. the index of the identity of the abstract index group is mapped to the identity of the multiplicative group of positive rationals. For the inverse of T we can change the roles of $\mathcal{A}_M$ and $\mathcal{R}_M$ in the reduced definition, i.e., we have $\mathrm{ind}(T^{-1}) = 1/\mathrm{ind}(T)$. From the reduced definition we also find that for every positive rational a we can construct a QCA with index a.

(*ii*) For the tensor product $T \otimes \tilde{T}$ on possible different cell structures, it is clear that the right flow also decomposes into a tensor product $\mathcal{R}_{2x} \otimes \tilde{\mathcal{R}}_{2x}$. Since also the single cell dimensions are multiplied, the index is given by the product of the individual indices.

We assume, by regrouping of cells, that both T and $\tilde{T}$ are nearest neighbor QCAs on the cell structure $\{\mathcal{A}_x\}_{x\in\mathbb{Z}}$. The total right flow of $T \circ \tilde{T}$ can be calculated by

$$\begin{aligned}
\mathcal{R}_{2x}^{T\circ\tilde{T}} &= S(T \circ \tilde{T}(\mathcal{A}_{[2x,\dots,2x+3]}), \mathcal{A}_{[2x+2,\dots,2x+5]}) \\
&= S\Big(T(\underbrace{S(\tilde{T}(\mathcal{A}_{[2x,\dots,2x+3]}), \mathcal{A}_{[2x+1,\dots,2x+4]})}_{=\mathcal{A}_{2x+1}\otimes\mathcal{A}_{2x+2}\otimes\tilde{\mathcal{R}}_{2x+2}}), \mathcal{A}_{[2x+2,\dots,2x+5]}\Big) \\
&= \mathcal{R}_{2x+1} \vee \underbrace{S(T(\tilde{\mathcal{R}}_{2x+2}), \mathcal{A}_{[2x+2,\dots,2x+5]})}_{\cong\tilde{\mathcal{R}}_{2x+2}} \\
&\cong \mathcal{R}_{2x+1} \otimes \tilde{\mathcal{R}}_{2x+2}\,.
\end{aligned}$$

For the index we get

$$\mathrm{ind}(T \circ \tilde{T}) = \frac{r(2x+1)\tilde{r}(2x+2)}{d(2x+2)d(2x+3)} = \mathrm{ind}(T)\mathrm{ind}(\tilde{T})\,. \tag{3.12}$$

For the shift τ_d it is easy to compute that $\mathcal{R} \cong \mathcal{M}_{d^2}$, i.e. $\mathrm{ind}(\tau_d) = d$, holds.

(*iii*) When we have $\mathrm{ind}(T) = 1$ it is clear from the local implementation scheme of Theorem 3.6 that reversing the local unitaries (in appropriate order) near the origin of the lattice will do the job. Otherwise, it is also clear that the composition of the isomorphisms between the different cell structures can not be reversed on a strictly finite region, since the cell structures at the boundaries do not match.

(*iv*) First regroup cells, such that both QCAs are nearest neighbor QCAs. Then for both QCAs we find blockwise unitary transformations between different cell structures. When the cell structure in the intermediate step is the same for both QCAs, i.e. when their indices are equal, the corresponding unitaries can be continuously deformed into each other. Otherwise, the cell structure must also be converted which is, according to the last paragraph, not a local operation.

■

In particular, the Theorem tells us that all possible indices can be generated by suitable tensor products of left and right shifts (*conditional* shifts). By multiplying a QCA with a conditional shift, every QCA can be reduced to one with

trivial index, i.e., up to a conditional shift all QCAs can be locally implemented in a Margolus partitioning scheme, analogous to the result of Kari for classical cellular automata [Kar96]. The ancillary space in the general case is therefore only required as work space for the shift operations. Also the shift operations are the only ones which cannot be locally deformed to the identity, except they are composed in a suitable way, e.g. $\tau_d \otimes \tau_d^{-1}$.

3.4 Higher Dimensional Cases

In higher lattice dimensions the task is much more challenging because there is more freedom for the flow of information. Without translation invariance there is no reason that a locally calculated information flow is constant throughout the lattice. For the one dimensional case, one can argue that for a strict reversible dynamics "putting something in" on one side of a finite region requires "something coming out" on the opposite side. Otherwise, information would get lost, which is contradictorily to the reversibility. Of course, in higher dimensions there is no unique "opposite" side and, since we more or less just formalized the previous argument, the results of the one dimensional case cannot be fully generalized to higher dimensions. Therefore we assume translation invariance in this Section.

But, even when we assume that translation invariance holds, the constructions are much more subtle, since the overlaps of the images of different cells are in general much more complicated. Indeed, we are not able to generalize our results from one to more dimensions. Nevertheless we can look for special cases, where we find schemes for local implementations without ancillary systems, e.g. for some QCAs with von Neumann neighborhood, or schemes for decompositions into conditional shifts and local unitaries.

All these special cases, which will be described in the following subsections hint that the index in higher lattice dimensions has to be defined for each lattice direction individually, e.g. we get different indices when looking in vertical or horizontal direction, respectively. A possible scheme would be to make periodic boundary conditions in all but one lattice direction (a "cylinder") leading to an effectively one-dimensional QCA for which the index can be computed. But for a good definition this should not depend on the size of the boundary conditions, the only restriction should be that these are wide enough such that the neighborhood scheme is regular (see Lemma 2.9), but unfortunately we have not been able to prove this in the general case.

The local implementability depends crucially on the properties of the single cell support algebras. In [SW04] (see also Lemma 5.5) it is shown that a QCA can be implemented by commuting unitaries, if all single site support algebras apart from the centered one are abelian. The results we present here depend on whether the algebras commute, i.e., they do not have to abelian in the first place.

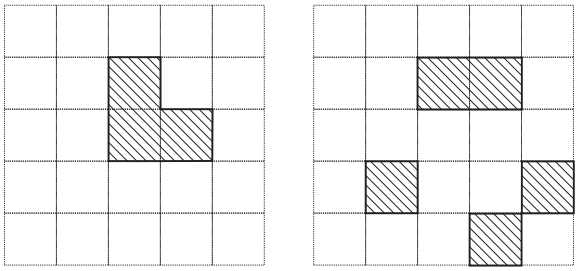

Figure 3.2: *Two examples of neighborhood schemes in 2D with unique difference vectors.*

3.4.1 Commuting Support Algebras

In this Subsection we describe a decomposition of a QCA step into conditional shifts and one-site transformations, which works in every lattice dimension, if the single-site support algebras

$$\mathcal{D}_x = S(T(\mathcal{A}_0), \mathcal{A}_x) \subset \mathcal{A}_x \,, \tag{3.13}$$

considered as subalgebras of the same matrix algebra, commute.

Proposition 3.8 *Let T be a QCA such that all algebras $\tau^{-x}\mathcal{D}_x \subset \mathcal{A}_0$ for $x \in \mathcal{N}$ commute pairwise. Then these are isomorphic to full matrix algebras and the QCA can be implemented by a one-site operation and a conditional shift.*

Proof: Note that the image of $\mathcal{A}_0$ is contained in the supports, i.e.

$$T(\mathcal{A}_0) \subset \bigotimes_{x\in\mathcal{N}} \mathcal{D}_x \,, \tag{3.14}$$

holds. A dimension count, similar to the information flows in 1D, then shows that $\bigotimes_{x\in\mathcal{N}} \tau^{-x}\mathcal{D}_x \cong \mathcal{A}_0$. Therefore, we have $\mathcal{D}_x \cong \mathcal{M}_{s(x)}$ with $\prod s(x) = d$. The QCA can then be described by a one-site operation, decomposing $\mathcal{A}_0$ into the subalgebras $\tau^{-x}\mathcal{D}_x$, which are afterwards shifted to the desired position. ■

However, the commutation relations have to checked for each single QCA and often they will not be fulfilled. Nevertheless, in some cases the desired commutation relations follow directly from the form of the neighborhood scheme. This will be described in the rest of this Subsection. We say a subset $\Lambda \subset \mathbb{Z}^s$ has unique difference vectors, if for $x, x', y, y' \in \Lambda$ the equation $x - y = x' - y' \neq 0$ implies that $x = x'$ and $y = y'$ hold (see Firgure 3.2 for examples).

Lemma 3.9 *Let T be a QCA with unique differences neighborhood. Then all the one-site support algebras $\tau^{-x}\mathcal{D}_x \subset \mathcal{A}_0$, shifted back to the origin, commute pairwise.*

Proof: Because of the translational invariance of T we have

$$\tau^{-x}\mathcal{D}_x = \tau^{-x}S(T(\mathcal{A}_0), \mathcal{A}_x) = S(T(\mathcal{A}_{-x}), \mathcal{A}_0).$$

Consider $x, y \in \mathcal{N}$ with $x \neq y$. Of course, $T(\mathcal{A}_{-x})$ and $T(\mathcal{A}_{-y})$ commute and we have to show that this holds for $\tau^{-x}\mathcal{D}_x$ and $\tau^{-y}\mathcal{D}_y$. Therefore, we verify that the overlap of $T(\mathcal{A}_{-x})$ and $T(\mathcal{A}_{-y})$ is contained in $\mathcal{A}_0$. So consider $z \in (-x + \mathcal{N}) \cap (-y + \mathcal{N})$ which is equivalent to $z + x, z + y \in \mathcal{N}$. Then we have $(z + x) - (z + y) = x - y \neq 0$ and the unique difference vectors of $\mathcal{N}$ imply $z + x = x$ and $z + y = y$ which gives $z = 0$. With Lemma A.1 the desired result follows. ■

Such a decomposition into one-site rotations and conditional shifts allows to define an index for the QCA. Of course, the index of the one-site rotations is trivial, and the index of the conditional shifts can be generalized from the one-dimensional case by looking towards different lattice directions. As an example, let us take a QCA with cell dimension 6 where in each step a qubit system is translated by one position to the right and a qutrit system by one position to the top. Then the index in horizontal direction is given by 1/3 and in vertical direction by 1/2.

3.4.2 Von Neumann Neighborhood

In the general scheme of [ANW08] a QCA on a two dimensional lattice with nearest neighbor interactions requires four layers of block unitary transformations. In this Subsection we look for examples for which a scheme with only two layers exists[3]. In these cases we can also quantify the amount of ancillary space which is needed for the local implementation. For this purpose we will restrict ourselves to the case of von Neumann neighborhoods, i.e., only the direct neighbors interact and not the diagonal ones (see Figure 2.1), but it is easy to see that these neighborhoods do not have unique difference vectors. Even with this restriction we need additional commutation relations to make our scheme work, however, compared to the previous Subsection, the centered support algebra does not necessarily have to commute with the other ones.

[3]Our scheme corresponds to a structure theorem in an earlier version of [SW04], which unfortunately turned out to be false. Here we describe special cases where the theorem still holds.

As in the previous Subsection we define the one-site support algebras by

$$\mathcal{D}_x = S(T(\mathcal{A}_0), \mathcal{A}_x)\,. \tag{3.15}$$

It is clear by the arguments from above, that $\mathcal{D}_{(0,1)}$ and $\mathcal{D}_{(0,-1)}$ commute, when considered as subalgebras of $\mathcal{M}_d$, and similarly for $\mathcal{D}_{(1,0)}$ and $\mathcal{D}_{(-1,0)}$. But in general nothing is known about the commutation relations of, e.g., $\mathcal{D}_{(1,0)}$ and $\mathcal{D}_{(0,1)}$.

Similar to the case of the definition of the flows, we need to group cells together. We define a "box" or "plaquette" of lattice vectors by

$$\boxplus := \left\{ \begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix} \right\}, \tag{3.16}$$

and we consider the support algebras of this box in the shifted boxes, e.g.

$$\mathcal{B}_{\nwarrow} = S\left(T(\mathcal{A}(\boxplus)), \mathcal{A}(\boxplus + \nwarrow)\right), \tag{3.17}$$

where $\nwarrow = (-1,1)$, and analogously for $\nearrow = (1,1), \swarrow = (-1,-1), \searrow = (1,-1)$.

With these definitions we get the following statement.

Theorem 3.10 *Let T be a QCA with von Neumann neighborhood such that all the one-site algebras $\tau^{-x}\mathcal{D}_x$ for $x \neq 0$ commute elementwise. Then the support algebras $\tau^{-y}\mathcal{B}_y$ for $y \in \{\nwarrow, \nearrow, \searrow, \swarrow\}$ commute elementwise and are isomorphic to full matrix algebras, i.e. $\mathcal{B}_y \cong \mathcal{M}_{d(y)}$ with $\prod_y d(y) = d^4$.*

Proof: The overlap of $T(\mathcal{A}(\boxplus + y))$ and $T(\mathcal{A}(\boxplus - y))$ for $y \in \{\nwarrow, \nearrow, \searrow, \swarrow\}$ is contained in $\boxplus$, therefore the support algebras, i.e. $\tau^{-y}\mathcal{B}_y$ and $\tau^{y}\mathcal{B}_{-y}$, commute by the arguments from the previous sections. Let us therefore consider the algebras $\tau^{\swarrow}\mathcal{B}_{\nearrow}$ and $\tau^{\searrow}\mathcal{B}_{\nwarrow}$ (see Figure 3.3). All other cases can be treated analogously. With Eq. (A.5) and by paying attention to the neighborhood scheme we get

$$\begin{aligned}
\tau^{\swarrow}\mathcal{B}_{\nearrow} &= S\left(T(\mathcal{A}(\boxplus - (1,1))), \mathcal{A}(\boxplus)\right) \\
&= \underbrace{S\left(T(\mathcal{A}_{(-1,0)}), \mathcal{A}_{(0,0)}\right)}_{=:X_1} \vee \underbrace{S\left(T(\mathcal{A}_{(0,-1)}), \mathcal{A}_{(0,0)}\right)}_{=:X_2} \vee \\
&\quad \vee \underbrace{S\left(T(\mathcal{A}_{(0,0)}), \mathcal{A}_{(0,0)} \otimes \mathcal{A}_{(1,0)} \otimes \mathcal{A}_{(0,1)}\right)}_{=:X_3}
\end{aligned}$$

and

$$\begin{aligned}
\tau^{\searrow}\mathcal{B}_{\nwarrow} &= S\left(T(\mathcal{A}(\boxplus + (1,-1))), \mathcal{A}(\boxplus)\right) \\
&= \underbrace{S\left(T(\mathcal{A}_{(1,-1)}), \mathcal{A}_{(1,0)}\right)}_{=:Y_1} \vee \underbrace{S\left(T(\mathcal{A}_{(2,0)}), \mathcal{A}_{(1,0)}\right)}_{=:Y_2} \vee \\
&\quad \vee \underbrace{S\left(T(\mathcal{A}_{(1,0)}), \mathcal{A}_{(0,0)} \otimes \mathcal{A}_{(1,0)} \otimes \mathcal{A}_{(1,1)}\right)}_{=:Y_3}
\end{aligned}$$

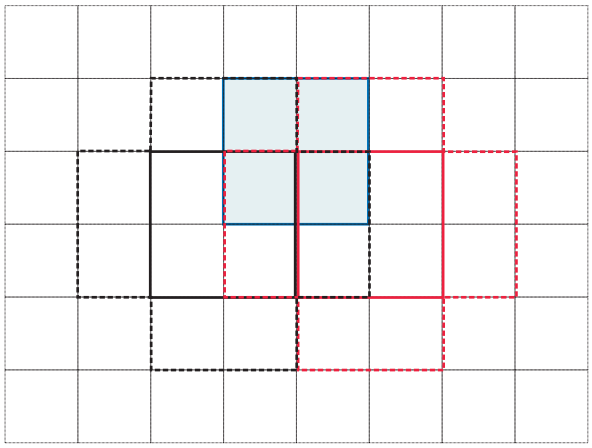

Figure 3.3: *It has to be shown that the support algebras in the blue box of the images of the black and the red box, respectively, commute.*

Now it is clear that the algebras commute, if all the generating algebras commute pairwise, i.e. $[X_i, Y_j] = 0$ for all i, j. For some of the algebras it is trivial that they commute because they are localized on different cells. Therefore we get

$$[X_1, Y_1] = [X_1, Y_2] = [X_2, Y_1] = [X_2, Y_2] = 0\,.$$

Furthermore, we have that the overlap between $T(\mathcal{A}_{(-1,0)})$ and $T(\mathcal{A}_{(1,0)})$ is contained in $\mathcal{A}_{(0,0)}$ and by Lemma A.1 the support algebras X_1 and Y_3 also commute. Similar statements show that $[X_3, Y_2] = [X_3, Y_3] = 0$ holds. The only remaining commutation relations are $[X_3, Y_1]$ and $[X_2, Y_3]$. But we have that $Y_1 = \tau^{(1,-1)}\mathcal{D}_{(0,1)}$ and with Eq. (A.4) we have $X_3 \subset \mathcal{D}_{(1,0)} \otimes S(T(\mathcal{A}_{(0,0)}), \mathcal{A}_{(0,0)} \otimes \mathcal{A}_{(0,1)})$, and by the assumption that the $\mathcal{D}_x$ commute, these algebras commute, too. Analogously, the algebras X_2 and Y_3 commute and therefore all the support algebras $\mathcal{B}_y$.

Since T is an automorphism, the algebras $\tau^{-y}\mathcal{B}_y$ together span the algebra $\mathcal{A}(\boxplus)$, and all of them have trivial center (compare the arguments for the right and left flow). So they are isomorphic to full matrix algebras and the dimensions multiply to the dimension of $\mathcal{A}(\boxplus)$. ■

Theorem 3.10 tells us that a QCA which fulfills all the assumptions can be implemented with two layers of block unitary transformations. These unitaries act on a plaquette of cells, i.e. a 2×2-block. The blocks of the second layer are translated by a diagonal lattice vector such that a plaquette of the second layer overlaps with four plaquettes of the first layer. The amount of ancillary space can again be computed by the dimensions of the $\mathcal{B}_y$, e.g., there is no ancilla system required, if all of them are isomorphic to $\mathcal{M}_d$.

Unfortunately, it is not clear that all QCAs with von Neumann neighborhood fulfill the required commutation relations. As mentioned above, we know that $\mathcal{D}_x$ and $\mathcal{D}_{-x}$ commute, but there is in general nothing known about the remaining commutation relations. This can only be done by imposing further restrictions on the QCA rule, e.g., the commutation relations are fulfilled, if one of the cells, except for the centered one, is not contained in the minimal neighborhood scheme. It can also be verified that the commutation relations hold in the case of Clifford QCAs, which are described in the following Chapter.

Furthermore, the information flow of the QCA is described by the dimensions of the $\mathcal{B}_y$. Therefore we can define the indices in vertical and horizontal direction by

$$\mathrm{ind}_{\uparrow}(T) = \frac{d(\nwarrow)d(\nearrow)}{d^2} \tag{3.18}$$

$$\mathrm{ind}_{\rightarrow}(T) = \frac{d(\nearrow)d(\searrow)}{d^2}\,. \tag{3.19}$$

From this definition it is also clear that the QCAs with trivial index, i.e. $\mathrm{ind}_{\uparrow}(T) = \mathrm{ind}_{\rightarrow}(T) = 1$ are exactly the QCAs which can be locally implemented without any ancillary space and which can be locally deformed to the identity.

3.4.3 QCAs with 2×2-Neighborhood and $d = 2$

When one is looking for examples of QCAs in two lattice dimensions, one will, of course, try to use small neighborhood schemes and small single cell dimensions. But there should also be some space for doing non trivial operations and, since we already clarified the structure of QCAs with some restrictions on the neighborhood scheme, we should go beyond these constraints. The simplest neighborhood scheme, which fulfills neither the unique differences assumptions nor is contained in a von Neumann neighborhood, is a 2×2-neighborhood, e.g. the box $\boxplus$ from above. When we further assume that the single cell dimension is given by $d = 2$, we get the following No-Go-Theorem:

Theorem 3.11 *There exists no two-dimensional QCA with single cell dimension $d = 2$ such that the minimal neighborhood scheme is given by $\boxplus$.*

Proof: Consider again the one-site support algebras $\mathcal{D}_x = S(T(\mathcal{A}_0), \mathcal{A}_x) \subset \mathcal{M}_2$. Because the neighborhood scheme $\boxplus$ should be minimal, we must have that $\mathcal{D}_x \neq \mathbb{C}\mathbb{1}$ for all $x \in \boxplus$. The only remaining subalgebras of $\mathcal{M}_2$ are then the abelian algebra, isomorphic to the diagonal matrices, and the full matrix algebra $\mathcal{M}_2$ itself. From the usual arguments from above the algebras $\mathcal{D}_{(0,0)}$ and $\mathcal{D}_{(1,1)}$ have to commute, as well as $\mathcal{D}_{(1,0)}$ and $\mathcal{D}_{(0,1)}$, and because none of them is trivial, they all have to be abelian. The tensor product $\bigotimes_x \mathcal{D}_x$ is then also abelian, which is a contradiction because it must contain an isomorphic copy of $\mathcal{M}_2$. ■

When we only assume that the neighborhood scheme is contained in $\boxplus$, we also have to study the cases where the minimal neighborhood is smaller, which leads always to a neighborhood scheme with unique differences. Since for $d = 2$ we do not have any subcell structure only the trivial QCAs, i.e. shifts and on-site rotations remain.

3.5 Conclusions and Outlook

We have introduced an index theory for local automorphisms on the quasi-local algebra, i.e., in the case of translation symmetry this class complies exactly with the class of quantum cellular automata, as defined in Chapter 2. For each QCA, or local automorphism, we have defined the information flow to the right and to the left, respectively, in terms of the matrix dimension of the corresponding parts of the image of local subalgebras. We have shown that this quantity, normalized with the local cell dimension, is constant throughout the chain. In particular, we have found a global quantity which is locally and therefore easily computable, and we identified this with the index of the QCA. We have shown that the index is a positive rational number for every QCA, which is multiplicative under composition of QCAs, i.e., the index is (as a map) a homomorphism from the group of QCAs into the multiplicative group of positive rationals. Especially, every QCA can be decomposed into a conditional shift and a QCA with trivial index.

We have also established an alternative approach to [ANW08] for a local implementation scheme of QCAs, where the size of the required ancilla space can be computed from the index. In particular, all QCAs with trivial index do not need an additional ancillary system for a local implementation in the form of a Margolus partitioning scheme. This shows that in the general approach the ancilla system is, at least in one lattice dimension, only needed as local work space for the shift operations. The subgroup of QCAs with trivial index is also interesting from various other points of view. For instance, this is exactly the subgroup which allows a local deformation to the identity and which can be decoupled by a local transformation into independent dynamical systems on the half-chains.

In higher lattice dimensions it seems that corresponding results are only expected in the translationally invariant case. But even with this restriction we could not fully generalize our theory. We have studied special cases of neighborhood schemes, especially schemes with unique difference vectors and von Neumann neighborhoods, where some of the results could be transferred.

A more general index theory in higher dimensions is left open for future work as well as an index theory for approximately local automorphisms, which may be possible by a further study of the Jones index.

Chapter 4

Clifford Quantum Cellular Automata

We study reversible quantum cellular automata with the restriction that these are also Clifford operations. This means that tensor products of Pauli operators (or discrete Weyl operators) are mapped to tensor products of Pauli operators. Therefore Clifford quantum cellular automata are induced by symplectic cellular automata in phase space. We characterize these symplectic cellular automata and find that all possible local rules must be, up to some global shift, reflection invariant with respect to the origin. In the one dimensional case we also find that every uniquely determined and translationally invariant stabilizer state can be prepared from a product state by a single Clifford cellular automaton timestep, thereby characterizing these class of stabilizer states, and we show that all 1D Clifford quantum cellular automata are generated by a few elementary operations. We also show that the correspondence between translationally invariant stabilizer states and translationally invariant Clifford operations holds for periodic boundary conditions.

Most of the results of this Chapter have been published in a joint paper [SVW08] with Dirk M. Schlingemann and Reinhard F. Werner.

4.1 Introduction

As already mentioned, quantum cellular automata are a versatile tool for many tasks in quantum information, e.g. universal quantum computation and simulation of strongly interacting quantum systems. In particular, this means that many QCAs do not allow for an efficient classical description, i.e. on a classical computer the resources needed for the simulation of the QCA grow exponentially with the system size, because otherwise all the tasks of the QCA could be executed on a classical computer. Of course, this behavior causes trouble for many interesting questions about QCAs which one would like to study, e.g. asymptotic

behavior, invariant states or entanglement generation. It is therefore helpful to have some class of QCAs, which are easier to handle but still show interesting behavior apart from classical cellular automata, such that they can serve as testing ground for general ideas about QCAs. This Chapter is concerned with such a characterization, namely of the special class of Clifford quantum cellular automata (CQCAs for short), in which the elementary time step is given by a "Clifford gate", meaning that it takes tensor products of Pauli matrices to tensor products of other Pauli matrices.

In the theory of gate model computation, and for the one-way quantum computation model, a detailed analysis of what can be done with Clifford operations alone turned out to be very useful, even though – as the downside of allowing an efficient classical description – such gates alone do not allow universal quantum computation. By analogy it is therefore clear that CQCAs do not comprise the full complexity of QCAs. What one can hope to get, however, is an interesting class of cellular automata, and some tools for understanding this class in great detail.

A similar analysis has been done with Gaussian quantum cellular automata in [KW07], e.g. the QCA describes a chain of harmonic oscillators with nearest neighbor couplings. For all these QCAs the Hilbert space of one elementary cell is infinite dimensional, and the QCA maps phase space translations, also referred to as Weyl operators, to phase space translations. In our approach we use elementary cells with a finite number of levels, which corresponds to replacing the continuous phase space by a discrete space.

Our formalism of CQCAs has indeed be used as a test model for the study of special cellular automaton questions. In [Güt08, Uph08] the structure of CQCAs which posses "gliders", i.e., observables which are preserved up to a shift, is analyzed. [Uph08] is also concerned with the asymptotic behavior starting from a translationally invariant product state and with the search for invariant states, i.e. states which do not change during the discrete time evolution.

4.1.1 Definition of Clifford Quantum Cellular Automata

According to the Definition 2.7 a quantum cellular automaton is a translationally invariant and local homomorphism on the quasi-local algebra. We have seen in Lemma 2.8 that the global rule is uniquely determined by its local rule which is just the restriction to observables which are localized in a single cell and that all valid local rules have to obey some commutation relations.

For special classes, the job of specifying a QCA via its local rule can be reduced still further, which is where the Clifford condition comes in. Let us assume now that we have a qubit system, so the local cell dimension is $p = 2$. For each local cell we thus have a basis for the observables, consisting of the identity and the three Pauli matrices, which we denote by X, Y and Z. By X_x etc. we denote the corresponding Pauli matrix belonging to the cell x. Finite tensor products

of Pauli matrices belonging to different sites, perhaps with a sign $\pm 1, \pm i$ will be referred to as *Pauli products*. These form a group, called the Pauli group. Then a *Clifford quantum cellular automaton* T is defined by the following condition: If A is any multiple of a Pauli product, so is $T(A)$. Clearly, this is equivalent to the property that one-cell Pauli operators are taken to Pauli products, which simplifies the local rule. Moreover, it suffices to specify $T(X_x)$ and $T(Z_x)$ for some x, because we can compute $T(Y_x) = T(iX_xZ_x) = iT(X_x)T(Z_x)$ via the homomorphism property. Hence a CQCA is defined in terms of just two Pauli products.

Example 4.1 For the one-dimensional lattice ($s = 1$), consider the relations

$$\begin{array}{lcccc} T(X_x) & = & & -Z_x & \\ T(Z_x) & = & Z_{x-1}\otimes & X_x & \otimes Z_{x+1} \end{array} \tag{4.1}$$

Let us verify that all requirements for a local rule are satisfied. To begin with each of the expressions on the right hand side, as a product of Pauli matrices, is hermitian with square one. These are all the required conditions related to just a single line, and are satisfied for any Pauli product with a sign ± 1. Next we have to verify the anti-commutation relation arising from applying a homomorphism T to the anti-commutation relation $XZ + ZX = 0$. Indeed, $T(X_x)T(Z_x) + T(Z_x)T(X_x) = -Z_{x-1} \otimes (Z_xX_x + X_xZ_x) \otimes Z_{x+1} = 0$. Hence the definition $T(Y_x) = iT(X_x)T(Z_x)$ again produces a hermitian operator with square , and the local rule is a homomorphism T_x into the algebra on the sites $x + \mathcal{N}$ with $\mathcal{N} = \{-1, 0, 1\}$. Finally, we have to check the commutation rules for the images of observables from neighboring sites. For example, we have $[T(X_x), T(Z_{x+1})] = -[Z_x, Z_x \otimes X_{x+1} \otimes Z_{x+2}] = 0$, and similarly $[T(Z_x), T(Z_{x+2})] = 0$. Perhaps the only non-trivial relation to check is

$$[T(Z_x), T(Z_{x+1})] = [Z_{x-1} \otimes X_x \otimes Z_{x+1}, Z_x \otimes X_{x+1} \otimes Z_{x+2}] = 0\,,$$

which holds because the factors on sites x and $x + 1$ both *anti*-commute.

In principle, we would also have to check the existence of an inverse for the automaton, which is actually given by $T^{-1}(X_x) = X_{x-1} \otimes Z_x \otimes X_{x+1}$ and $T^{-1}(Z_x) = -X_x$, but as was shown in [SW04] and in Subsection 2.2.2, this already follows from the homomorphism property. ◊

It is clear from this example that the search for CQCAs is now a combinatorial problem. We can first look for *self commuting* Pauli products, i.e., Pauli products, which commute with all translates of itself. Only these can appear on the right hand side of local rules. One can then check, for any pair X', Z' of such products, whether they anti-commute, while all proper translates of X' commute with Z'. In fact, we began our investigation by running this simple search program. We found, for example, that while there is a rich variety of self-commuting Pauli products only reflection symmetric products could appear in a local rule. This will indeed be shown in full generality below.

4.1.2 Translationally Invariant Stabilizer States

Commuting sets of Pauli products also play a central role in the problem of determining so-called stabilizer states: these are pure states, which can be characterized by eigenvalue equations for Pauli products or, equivalently, by the condition that certain Pauli products have expectation ± 1. It is easy to check that Pauli products which simultaneously have sharp expectations ± 1 must commute. Now for the infinite lattice systems it is natural to ask which Pauli products A have the property that there is a unique pure state ρ of the infinite system, which has expectation 1 for A and all its translates.

As the simplest example, let us take $A = Z_x$, so we ask for states with $\langle Z_x \rangle = 1$ for all $x \in \mathbb{Z}^s$. Clearly, this defines the "all spins up" state, which is an infinite product state. A slightly more complex example uses the stabilizer operators $A = Z_{x-1} \otimes X_x \otimes Z_{x+1}$, which singles out the one-dimensional *cluster state*, whose higher dimensional analogs are used as the entanglement resource for universal one-way quantum computing [RB02].

Showing that these eigenvalue equations define a unique state of the infinite lattice is now very easy, by using the cellular automaton (4.1): Since this automaton maps Z_x to the required stabilizer operator, all existence and uniqueness problems for such a state are mapped to the corresponding trivial questions for the stabilizer operator Z_x. In other words, self-commuting Pauli products of the form $A = T(Z_x)$ for some CQCA T characterize a unique translation invariant cluster state. We will show later that (at least in one dimension) the converse is also true, so that there is a very close connection between stabilizer states and Clifford cellular automata.

4.1.3 Our Methods and Techniques

The definition of CQCAs given above applies only to qubit systems. However, all our results are also valid for higher dimensional cells, in particular cells of prime dimension[1] p. The role of the Pauli operators X and Z is then taken by the cyclic shift on $\mathbb{C}^p$, and the multiplication by a phase, i.e.

$$\begin{array}{rcl} X|q\rangle & = & |q+1\rangle \\ Z|q\rangle & = & \mathrm{e}^{2\pi i q/p}|q\rangle\,, \end{array} \tag{4.2}$$

where all ket labels q are taken modulo p. Products of these operators are called *Weyl operators*, and the appropriate definition of CQCAs requires that $T(X_x)$ and $T(Z_x)$ are both tensor products of Weyl operators. The necessary preliminaries on the Pauli group and Clifford operations in this extended setting, and the background concerning infinite lattice systems are provided in Subsection 4.2.1.

[1] In this Chapter the single cell dimension is denoted by p instead of d to emphasize that it is a prime number.

In order to utilize the translation symmetry one would like to use Fourier transform techniques. However, in the discrete structures an integral with complex phases makes no sense. It turns out, however, that a "generating function" technique does nearly as well. The analogue of the Fourier transform is then a Laurent-polynomial in an indeterminate variable, i.e., a polynomial with coefficients in the field $\mathbb{F} = \mathbb{Z}_p$ with both positive and negative powers. The salient facts about this structure will be provided in Subsection 4.2.3.

The description in terms of Laurent polynomials can also be adapted to lattices with periodic boundary conditions. This will be described in Section 4.4.

4.1.4 Outline and Summary of Results

In order to discuss general Clifford quantum cellular automata, that is, for arbitrary lattice and single cell dimension, we introduce in Section 4.2 the necessary mathematical tools. We first review the concept of discrete Weyl systems and (infinite) tensor products of them, thereby characterizing the underlying "phase space". We show that Clifford QCAs can be completely characterized in terms of classical symplectic cellular automata. We also introduce our Fourier transform techniques and study the structure of isotropic subspaces, because these play an essential role for the characterization of symplectic cellular automata and translationally invariant stabilizer states.

In Section 4.3 we will state our main results. We show that symplectic cellular automata can be identified with two-by-two matrices, which have Laurent-polynomials as matrix elements. We will find that the determinant of this matrix must be one and that the polynomials must be reflection invariant. In the one-dimensional case we state that every translationally invariant stabilizer state can be prepared out of a product state by a single CQCA step. Furthermore, we also specify the generators of all 1D QCAs.

Finally, we show in Section 4.4 that the close connection between translationally invariant stabilizer states and CQCAs also holds in the case of periodic boundary conditions even in every lattice dimension.

4.2 Mathematical Tools

We introduce some mathematical tools, which we will use to study Clifford QCAs. We start with a short repetition of finite Weyl systems, which generalize the Pauli operators to systems with prime number dimensions. These Weyl operators can be described by phase space vectors and Clifford operations are induced by symplectic transformations on the phase space. Since we are looking for translationally invariant operations, we also introduce some kind of Fourier transform.

4.2.1 Weyl Algebras

Each single cell in a QCA is given by a finite dimensional quantum system, so the observables on a single system can be described by matrices from the algebra $\mathcal{M}_p(\mathbb{C})$. A possible basis for this algebra is given by Weyl operators $\mathbf{w}(r,k) = X^r Z^k$, where X and Z are given by the generalized Pauli operators from equation (4.2). These operators fulfill the Weyl relations

$$\mathbf{w}(r_1 + r_2, k_1 + k_2) = \varepsilon^{-r_2 k_1} \mathbf{w}(r_1, k_1)\mathbf{w}(r_2, k_2)\,, \tag{4.3}$$

where $\varepsilon = \exp(2\pi \mathrm{i}/p)$ is the p^{th} root of unity. From this equation the commutation relation

$$\mathbf{w}(r_1, k_1)\mathbf{w}(r_2, k_2) = \varepsilon^{r_1 k_2 - r_2 k_1} \mathbf{w}(r_2, k_2)\mathbf{w}(r_1, k_1) \tag{4.4}$$

immediately follows. Obviously we get for $p = 2$ the standard Pauli operators from

$$X = \mathbf{w}(1,0)\,, \quad Y = i\mathbf{w}(1,1)\,, \quad Z = \mathbf{w}(0,1)\,, \tag{4.5}$$

and the Weyl operators are generalizations of the Pauli operators to higher dimensional spaces. The indices r and k are integers modulo p, so they are elements of the finite field $\mathbb{F} = \mathbb{Z}_p$. In infinite dimensional systems Weyl operators describe phase space translations and therefore we call the space $\mathbb{F}^2$ a discrete phase space.

Building a tensor product of Weyl operators means that we must assign a phase space vector $\xi(x) = (\xi_+(x), \xi_-(x)) \in \mathbb{F}^2$ to each lattice point $x \in \mathbb{Z}^s$, so ξ is a mapping from $\mathbb{Z}^s$ into $\mathbb{F}^2$ and we denote for the tensor product

$$\mathbf{w}(\xi) = \bigotimes_{x \in \mathbb{Z}^s} \mathbf{w}(\xi(x))\,. \tag{4.6}$$

This infinite tensor product is well defined, if there are only finitely many of the Weyl operators different from $= \mathbf{w}(0)$. For a mapping $\xi : \mathbb{Z}^s \to \mathbb{F}^2$ we have that only finitely many x with $\xi(x) \neq 0$ are allowed, so the support of ξ is finite. The set of such functions describes the global system and is identified with the global phasespace Ξ_s. We denote the finitely supported functions from $\mathbb{Z}^s$ to $\mathbb{F}$ by $C_{\mathbb{F}}(\mathbb{Z}^s)$ and we have $\Xi_s = C_{\mathbb{F}}(\mathbb{Z}^s)^2$. The corresponding Weyl operators generate an algebra and, by restricting the support of the functions to some finite subset $\Lambda \in \mathbb{Z}^s$, we get a finite dimensional algebra $\mathcal{A}(\Lambda) = \bigotimes_{x \in \Lambda} \mathcal{M}_p(\mathbb{C})$, also called the local algebra of Λ. By taking the union of these algebras over all finite subsets of $\mathbb{Z}^s$ and taking the closure (in operator norm) we get the usual quasi-local C^*-algebra $\mathcal{A}(\mathbb{Z}^s)$.

The local structure is accompanied by the symmetry group of lattice translations. For each lattice translation $x \in \mathbb{Z}^s$ an automorphism τ^x is defined by

$$\tau^x \mathbf{w}(\xi) = \mathbf{w}(\alpha^x \xi)\,. \tag{4.7}$$

where α^x is the translation of phase space vectors. Given a phase space vector ξ, the translated vector is $(\alpha^x\xi)(y) = \xi(y-x)$. So the automorphism τ^x shifts the position of each tensor factor by x. It follows directly from (4.7) that the homomorphism property $\tau^{x+y} = \tau^x\tau^y$ holds. Furthermore, the automorphism τ^x maps the local algebra $\mathcal{A}(\Lambda)$ onto $\mathcal{A}(\Lambda + x)$.

The Weyl relations of a single system completely determine the relations of the global system which are given by

$$\mathbf{w}(\xi+\eta) = \varepsilon^{\beta(\xi,\eta)}\mathbf{w}(\xi)\mathbf{w}(\eta) \ , \tag{4.8}$$

where we have introduced the bilinear form $\beta(\xi,\eta) := \sum_{x\in\mathbb{Z}^s} \xi_+(x)\eta_-(x)$. The adjoint of a Weyl operator is given by

$$\mathbf{w}(\xi)^* = \varepsilon^{-\beta(\xi,\xi)}\mathbf{w}(-\xi) \tag{4.9}$$

which is due to the unitarity of the Weyl operators.

Since commutation relations are essential for validating possible local rules of quantum cellular automata, the commutation relations of Weyl operators are most important for us. We get

$$\mathbf{w}(\eta)\mathbf{w}(\xi) = \varepsilon^{\sigma(\xi,\eta)}\mathbf{w}(\xi)\mathbf{w}(\eta) \ , \tag{4.10}$$

where $\sigma(\xi,\eta) := \beta(\xi,\eta) - \beta(\eta,\xi)$ is the canonical symplectic form on Ξ_s. This means that two Weyl operators $\mathbf{w}(\xi)$ and $\mathbf{w}(\eta)$ are commuting if and only if $\sigma(\xi,\eta) = 0$ (and for $p = 2$ they anti-commute if $\sigma(\xi,\eta) = 1$). In particular, an abelian algebra of Weyl operators is given by a subspace of Ξ_s on which the symplectic form vanishes. Such a subspace is called isotropic and a maximally abelian algebra corresponds to a maximally isotropic subspace.

4.2.2 Clifford Quantum Cellular Automata

As already mentioned a Clifford quantum cellular automaton is a QCA which maps Weyl operators to multiples of Weyl operators, which are in our case tensor products of single cell Weyl operators, so we have the relation (the "Clifford condition")

$$T(\mathbf{w}(\xi)) = \vartheta(\xi)\mathbf{w}(\mathbf{t}\xi) \tag{4.11}$$

with a mapping $\mathbf{t}$ on the phase space Ξ_s and some phase valued function $\vartheta : \Xi_s \to \mathcal{U}(1) = \{z \in \mathbb{C} || z| = 1\}$. Since T is an automorphism we find with equation (4.10) that $\mathbf{w}(\mathbf{t}\xi)\mathbf{w}(\mathbf{t}\eta) = \varepsilon^{\sigma(\eta,\xi)}\mathbf{w}(\mathbf{t}\eta)\mathbf{w}(\mathbf{t}\xi)$ holds, so we have $\sigma(\mathbf{t}\xi,\mathbf{t}\eta) = \sigma(\xi,\eta)$ or in other words $\mathbf{t}$ is a symplectic transformation.

For reversible operations the Clifford condition is in general equivalent to the Weyl covariance (for general theory on covariant channels we refer to [Scu79] and for the special case of Weyl covariance to [Hol02, Hol04]) of the quantum channel:

Proposition 4.2 *An automorphism T on the Weyl algebra $\mathcal{A}(\mathbb{Z}^s)$ fulfills the Clifford condition (4.11) if and only if the Weyl covariance*

$$T(\mathbf{w}(\eta)A\mathbf{w}(\eta)^*) = \mathbf{w}(\mathbf{t}\eta)T(A)\mathbf{w}(\mathbf{t}\eta)^* \quad \forall \eta \in \Xi_s \tag{4.12}$$

holds for all operators $A \in \mathcal{A}(\mathbb{Z}^s)$ and some symplectic transformation $\mathbf{t}$.

Proof: Because the Weyl operators form a basis of $\mathcal{A}(\mathbb{Z}^s)$ we just have to insert $\mathbf{w}(\xi)$ for some $\xi \in \Xi_s$ in the covariance condition, which yields the equation $\varepsilon^{\sigma(\xi,\eta)}T(\mathbf{w}(\xi)) = \mathbf{w}(\mathbf{t}\eta)T(\mathbf{w}(\xi))\mathbf{w}(\mathbf{t}\eta)^*$. If T is a Clifford automorphism we have already seen that $\mathbf{t}$ is a symplectic transformation and obviously fulfills this equation. In the inverse direction we get that $T(\mathbf{w}(\xi))$ must be a multiple of $\mathbf{w}(\mathbf{t}\xi)$, because the relation must hold for all $\eta \in \Xi_s$ and the symplectic form is non degenerate (note that the support of the phase space vectors is finite and that $\mathbf{t}$ maps therefore finitely supported vectors to finitely supported vectors, so the commutation relations can be checked in a finite dimensional space). ■

Since a QCA is a translationally invariant automorphism on the quasilocal algebra, it suffices that the Clifford condition holds for the local rule, e.g. the QCA restricted to operators which are localized in a single cell. Furthermore, because of the Weyl relations on a single cell, we only need to specify the image of the Weyl operators $\mathbf{w}(1,0)$ and $\mathbf{w}(0,1)$. To some extend we are free in the choice of the phases $\vartheta(1,0), \vartheta(0,1) \in \mathcal{U}(1)$, since these phases do not interfere with the commutation relations for the local rule. The only condition is that some power of a Weyl operator is always equal to (we will specify this below), and so these phases must be some roots of unity. The two phases $\vartheta(1,0)$ and $\vartheta(0,1)$ completely determine the function ϑ.

Of course $\mathbf{t}$ and ϑ must be translationally invariant, because T is translationally invariant. Using the homomorphism property of the QCA and equation (4.8) we get $\vartheta(\xi+\eta)\mathbf{w}(\mathbf{t}(\xi+\eta)) = \vartheta(\xi)\vartheta(\eta)\varepsilon^{\beta(\xi,\eta)-\beta(\mathbf{t}\xi,\mathbf{t}\eta)}\mathbf{w}(\mathbf{t}\xi+\mathbf{t}\eta)$, so – because the Weyl operators form a basis – the transformation $\mathbf{t}$ must be linear and the phase function must fulfill

$$\vartheta(\xi+\eta) = \vartheta(\xi)\vartheta(\eta)\varepsilon^{\beta(\xi,\eta)-\beta(\mathbf{t}\xi,\mathbf{t}\eta)}\ , \tag{4.13}$$

which enables us to calculate the phase $\vartheta(\xi)$ for each $\xi \in \Xi_s$, if the local rule and therefore $\mathbf{t}$ and the phases $\vartheta(1,0)$ and $\vartheta(0,1)$ are given. In total we get the following theorem:

Theorem 4.3 *If T is a Clifford quantum cellular automaton (equation (4.11)) on the Weyl algebra $\mathcal{A}(\mathbb{Z}^s)$, then $\mathbf{t}$ is a translationally invariant linear symplectic transformation ("symplectic cellular automaton") and the phase function ϑ fulfills equation (4.13).*

This means that we are able to study Clifford QCAs – up to some phase function – in terms of a classical cellular automaton on the phase space Ξ_s. It is well known that Clifford operations allow an efficient classical description, which in the case of QCAs turned out to be the group of classical symplectic cellular automata. In the rest of the paper we will study the structure of this kind of cellular automata, thereby characterizing the structure of CQCAs.

We would like to give a closed expression for the phase function ϑ, but this has to be done in dependence of the cell dimension. First we consider the case $p \neq 2$. Then all Weyl operators fulfill $\mathbf{w}(\xi)^p =$ and because of $T(\ ) =$ the phase $\vartheta(\xi)$ must be a p^{th} root of unity. So we can write $\vartheta(\xi) = \varepsilon^{\varphi(\xi)}$ with a function $\varphi : \Xi_s \to \mathbb{F}$, which then has to fulfill $\varphi(\xi+\eta) = \varphi(\xi) + \varphi(\eta) + \beta(\xi,\eta) - \beta(\mathbf{t}\xi, \mathbf{t}\eta)$. This equation determines the function $\varphi(\xi)$ up to some linear functional $\lambda(\xi)$, which is given by the choice of the phases $\varphi(1,0)$ and $\varphi(0,1)$. The bilinear form $\beta(\xi,\eta) - \beta(\mathbf{t}\xi, \mathbf{t}\eta)$ is symmetric, because $\mathbf{t}$ is a symplectic transformation. If $p \neq 2$ we may divide by 2 and the general solution is $\varphi(\xi) = \frac{1}{2}(\beta(\xi,\xi) - \beta(\mathbf{t}\xi, \mathbf{t}\xi)) + \lambda(\xi)$.

The case of qubits ($p = 2$) is slightly more complicated because the Weyl operators fulfill $\mathbf{w}(\xi)^2 = (-1)^{\beta(\xi,\xi)}$. So the phase function must fulfill $\vartheta(\xi) = \mathrm{i}^{\varphi(\xi)}$ with $\varphi : \Xi_s \to \mathbb{Z}_4$. We replace the form $\beta : \Xi_s \times \Xi_s \to \mathbb{Z}_2$ by the bilinear form $\tilde{\beta} : \Xi_s \times \Xi_s \to \mathbb{Z}_4$, which is formally given by $\tilde{\beta} = 2\beta$, so the values of $\tilde{\beta}$ are even elements of $\mathbb{Z}_4$ and the Weyl relation becomes $\mathbf{w}(\xi+\eta) = \mathrm{i}^{\tilde{\beta}(\xi,\eta)}\mathbf{w}(\xi)\mathbf{w}(\eta)$. This means that φ fulfills $\varphi(\xi+\eta) = \varphi(\xi) + \varphi(\eta) + \gamma(\xi,\eta)$ with the form $\gamma(\xi,\eta) = \tilde{\beta}(\xi,\eta) - \tilde{\beta}(\mathbf{t}\xi, \mathbf{t}\eta)$. This form is symmetric, so in the decomposition $\gamma(\xi,\eta) = \sum_{i,j} \gamma_{ij}\xi_i\eta_j$ we have $\gamma_{ij} = \gamma_{ji}$ and all these elements are even. We can find γ_i with $\gamma_{ii} = 2\gamma_i$, but this choice is not unique in $\mathbb{Z}_4$ and corresponds exactly to the freedom in the choice of the phases $\vartheta(1,0)$ and $\vartheta(0,1)$. The solution for φ is then given by $\varphi(\xi) = \sum_{i<j} \gamma_{ij}\xi_i\xi_j + \sum_i \gamma_i\xi_i$ (note that $\xi_i \in \{0,1\}$ and so $\xi_i^2 = \xi_i$ holds).

4.2.3 Algebraic Fourier Transform

We would like to use Fourier transform techniques for the study of the structural properties of symplectic CA, because of translational invariance, and because we know that this is very helpful for symplectic CA with continuous single cell phase space [KW07]. So we have to apply a Fourier transform to the functions $C_{\mathbb{F}}(\mathbb{Z}^s)$. But the values of these functions are in the finite field $\mathbb{F}$ and multiplying such a value with a complex number does not really match. It turns out that a slight modification of the usual Fourier transform does as well. For a function $f \in C_{\mathbb{F}}(\mathbb{Z}^s)$ we define

$$\hat{f}(u) = \sum_{x \in \mathbb{Z}^s} f(x) u^x \ , \tag{4.14}$$

with $u^x = u_1^{x_1} \cdots u_s^{x_s}$. Now the transformed function $\hat{f}$ is a polynomial or, more precisely, a Laurent-polynomial in the variables $u_1, \ldots, u_s$ with coefficients in $\mathbb{F}$.

The set of such polynomials will be denoted by $\mathcal{P}_s = \mathbb{F}[u_1, \cdots, u_s, u_1^{-1}, \cdots, u_s^{-1}]$. Note that we have indeed polynomials, because the functions in $C_{\mathbb{F}}(\mathbb{Z}^s)$ are finitely supported. Equation (4.14) identifies functions of $C_{\mathbb{F}}(\mathbb{Z}^s)$ with polynomials in $\mathcal{P}_s$ and this identification is unique, so $C_{\mathbb{F}}(\mathbb{Z}^s)$ and $\mathcal{P}_s$ are isomorphic. The usual Fourier transform would require $u_n = e^{ik_n}$. We do not further specify the domain of the variables, and this approach can be seen as "generating function approach" or "algebraic Fourier transform".

The convolution $f \star h = \sum_x f(-x)\alpha^x h$ is a natural product[2] of functions in $C_{\mathbb{F}}(\mathbb{Z}^s)$. The invertible elements with respect to this operation are the functions which are supported on a single lattice point, e.g. $f = c\delta_x$ (δ_x is the Kronecker-delta) with $c \in \mathbb{F}$ and $x \in \mathbb{Z}^s$, and the unit element is δ_0. The nice fact about Fourier transform is that the convolution turns into a usual product which is also true for our algebraic version:

$$\widehat{f \star h} = \hat{f}\hat{h} \quad f, h \in C_{\mathbb{F}}(\mathbb{Z}^s) \; . \tag{4.15}$$

Note that the invertible polynomials are monomials[3], e.g. they are of the form u^x. Of course the unit element is the constant $1 = \hat{\delta}_0$. Another important operation is the reflection operation (or involution) $\overline{f}(x) := f(-x)$ for $f \in C_{\mathbb{F}}(\mathbb{Z}^s)$. Obviously the reflection preserves the convolution, e.g. $\overline{f \star h} = \overline{f} \star \overline{h}$, and for the transformed function we have $\hat{\overline{f}}(u) := \overline{\hat{f}}(u) = \hat{f}(u^{-1})$.

The phase space Ξ_s consists of two-dimensional tuples of functions from $C_{\mathbb{F}}(\mathbb{Z}^s)$ and all operations can be defined component-wise[4], so we get that the phase space is isomorphic to $\Xi_s \cong \mathcal{P}_s^2$. We would like to study the structure of symplectic CA in this polynomial space. The transformation of an operation $\mathbf{t} : \Xi_s \to \Xi_s$ is defined according to $\hat{\mathbf{t}}\hat{\xi} = \widehat{\mathbf{t}\xi}$, so $\hat{\mathbf{t}}$ is a mapping from $\mathcal{P}_s^2$ to $\mathcal{P}_s^2$. We introduce the symplectic form $\hat{\sigma} : \mathcal{P}_s^2 \times \mathcal{P}_s^2 \to \mathcal{P}_s$ by

$$\hat{\sigma}(\xi, \eta) = \overline{\xi_+}\eta_- - \overline{\xi_-}\eta_+ \; , \quad \xi, \eta \in \mathcal{P}_s^2 \; , \tag{4.16}$$

which can be written as $\hat{\sigma}(\xi, \eta) = \det(\overline{\xi}, \eta)$, where (ξ, η) denotes the 2×2-matrix

$$(\xi, \eta) = \begin{pmatrix} \xi_+ & \eta_+ \\ \xi_- & \eta_- \end{pmatrix} \tag{4.17}$$

with polynomial entries. The symplectic form $\hat{\sigma}$ is the best fitting symplectic form for symplectic CA, because it combines both the basic symplectic form σ as well as the translation invariance:

Proposition 4.4 *A linear operation* $\mathbf{t}$ *on the phase space* Ξ_s *is a symplectic cellular automaton, if and only if, the transformed operation* $\hat{\mathbf{t}}$ *leaves the symplectic form* $\hat{\sigma}$ *invariant.*

[2] With the convolution the set $C_{\mathbb{F}}(\mathbb{Z}^s)$ becomes a "commutative division ring".

[3] This will be different when we go to periodic boundary conditions.

[4] With the component-wise convolution the phase space is a two-dimensional $C_{\mathbb{F}}(\mathbb{Z}^s)$-module.

Proof: For this proof we introduce the form $\tilde{\sigma}(\xi,\eta) = \sigma(\xi,\alpha^{(\cdot)}\eta)$ for $\xi,\eta \in \Xi_s$. A straightforward computation shows that $\tilde{\sigma}(\xi,\eta) = \overline{\xi_+} \star \eta_- - \overline{\xi_-} \star \eta_+$ holds. This means we have $\widehat{\tilde{\sigma}(\xi,\eta)} = \hat{\sigma}(\hat{\xi},\hat{\eta})$, so $\hat{\sigma}$ is the Fourier transform of $\tilde{\sigma}$ and the invariance of $\tilde{\sigma}$ under some operation $\mathbf{t}$ is equivalent to the invariance of $\hat{\sigma}$ under $\hat{\mathbf{t}}$.

Now suppose $\mathbf{t}$ is a symplectic CA. Then we have for all $x \in \mathbb{Z}^s$ that

$$\tilde{\sigma}(\mathbf{t}\xi,\mathbf{t}\eta)(x) = \sigma(\mathbf{t}\xi,\alpha^x\mathbf{t}\eta) = \sigma(\mathbf{t}\xi,\mathbf{t}\alpha^x\eta) = \sigma(\xi,\alpha^x\eta) = \tilde{\sigma}(\xi,\eta)(x)$$

holds, because $\mathbf{t}$ is translationally invariant and preserves σ, so $\tilde{\sigma}$ is invariant under $\mathbf{t}$.

If $\mathbf{t}$ leaves $\tilde{\sigma}$ invariant, this holds also for $\sigma = \tilde{\sigma}(\cdot,\cdot)(0)$, and because of this $\sigma(\mathbf{t}\xi,\alpha^x\mathbf{t}\eta) = \sigma(\xi,\alpha^x\eta) = \sigma(\mathbf{t}\xi,\mathbf{t}\alpha^x\eta)$ holds for all $x \in \mathbb{Z}^s$ and all $\xi,\eta \in \Xi_s$ and so $\mathbf{t}$ must commute with the translations α^x. ■

So we can characterize symplectic CA in "momentum space" by studying the linear transformations on $\mathcal{P}_s^2$ which leave the symplectic form $\hat{\sigma}$ invariant. In the subsequent we will mainly work in the polynomial space $\mathcal{P}_s$. Therefore we will just identify the phase space Ξ_s with $\mathcal{P}_s^2$ and we will omit the symbol $\hat{}$ for the Fourier transform of transformations.

4.2.4 Isotropic Subspaces

As we have already seen in Subsection 2.2.2, commutation relations are important for the verification of local rules of reversible QCAs, because a QCA is a homomorphism and preserves the algebraic structure. Especially the images of X_x and Z_x must be "self-commuting", meaning that $[T(X_x),T(X_y)] = 0 = [T(Z_x),T(Z_y)]$ holds for all $x,y \in \mathbb{Z}^s$. So the operators $T(X_x)$ generate a translationally invariant abelian algebra. For Weyl operators translationally invariant abelian algebras correspond exactly to isotropic subspaces of $\mathcal{P}_s^2$ with respect to the symplectic form $\hat{\sigma}$ and these subspaces can be easily connected to translationally invariant stabilizer states. Therefore it is important for us to study the structure of these subspaces.

A $\mathcal{P}_s$-subspace[5] $\mathcal{I} \subset \mathcal{P}_s^2$ is called isotropic, if for all $(\xi,\eta) \in \mathcal{I}$ the symplectic form $\hat{\sigma}(\xi,\eta) = 0$ vanishes. An isotropic $\mathcal{P}_s$-subspace $\mathcal{I}$ is called maximally isotropic, if the relation $\hat{\sigma}(\xi,\eta) = 0$ for all $\xi \in \mathcal{I}$ implies that $\eta \in \mathcal{I}$ holds.

For us the form of the generators of isotropic, in particular maximally isotropic, $\mathcal{P}_s$-subspaces is important, because this is a substantial step for the characterization of local rules of CQCAs and translationally invariant stabilizer states. The following Lemma shows that a generator ξ of a singly generated maximally isotropic subspace is reflection invariant and that the components ξ_+ and ξ_- are

[5]More precisely one should say submodule, but we will use the more convenient word subspace.

coprime. We will call a polynomial $f \in \mathcal{P}_s$ (or a tuple of those) reflection invariant for some half integer lattice point $a \in \frac{1}{2}\mathbb{Z}^s$, if $f = u^{2a}\overline{f}$ holds. The greatest common divisor of two polynomials $f, h \in \mathcal{P}_s$ will be denoted by $\gcd(f, h)$. Note that the greatest common divisor is defined only up to invertible elements. We will simply write $\gcd(f, h) = 1$, if f and h are coprime.

Lemma 4.5

1. *If the subspace $\mathcal{P}_s\xi \subset \mathcal{P}_s^2$ is maximally isotropic, we have* $\gcd(\xi_+, \xi_-) = 1$.
2. *If the subspace $\mathcal{P}_s\xi \subset \mathcal{P}_s^2$ is maximally isotropic, ξ is reflection invariant to some point $a \in \frac{1}{2}\mathbb{Z}^s$.*
3. *Every reflection invariant polynomial ξ generates an isotropic $\mathcal{P}_s$-subspace $\mathcal{P}_s\xi$.*

Proof: Ad 1. Suppose $\mathcal{P}_s\xi$ is a maximally isotropic $\mathcal{P}_s$-subspace and $\gcd(\xi_+, \xi_-) = f$ is not invertible. So we can write $\xi = f\eta$ with $\gcd(\eta_+, \eta_-) = 1$, but $\eta \notin \mathcal{P}_s\xi$ since f is not invertible. But we have that $\hat{\sigma}(\xi, \eta) = f\hat{\sigma}(\xi, \xi) = 0$ holds, which is a contradiction to $\mathcal{P}_s\xi$ being maximally isotropic.

Ad 2. Suppose that $\mathcal{P}_s\xi$ is maximally isotropic. By 1 we have $\gcd(\xi_+, \xi_-) = 1$. Since $\hat{\sigma}(\overline{\xi}, \xi) = \xi_+\xi_- - \xi_-\xi_+ = 0$, it follows that $\overline{\xi} \in \mathcal{P}_s\xi$. So we have $\overline{\xi} = f\xi$ with some polynomial $f \in \mathcal{P}_s$. But for the reflected phase space vector $\overline{\xi}$ we also have that $\gcd(\overline{\xi}_+, \overline{\xi}_-) = 1$, so f must be invertible and therefore a monomial $f(u) = u^{-2a}$ for some $a \in \frac{1}{2}\mathbb{Z}^s$.

Ad 3. Suppose that $\xi = u^{2a}\overline{\xi}$ is reflection invariant. Then $\hat{\sigma}(\xi, \xi) = \hat{\sigma}(u^{2a}\overline{\xi}, \xi)$ $= u^{-2a}(\xi_+\xi_- - \xi_-\xi_+) = 0$ holds, and ξ generates an isotropic $\mathcal{P}_s$-subspace. ■

Example 4.6 Both $\xi_1 = (1 + u)\binom{0}{1}$ and $\xi_2 = \binom{1}{u+u^{-1}}$ are reflection invariant. The corresponding Weyl operators $\mathbf{w}(\xi_1) = Z_0 \otimes Z_1$ and $\mathbf{w}(\xi_2) = Z_{-1} \otimes X_0 \otimes Z_1$ are the same reading from the left and from the right ("palindromes"). Both phase space vectors generate isotropic subspaces. The subspace generated by ξ_2 is indeed maximally isotropic and the components $\xi_{2,+}$ and $\xi_{2,-}$ are coprime, whereas the subspace generated by ξ_1 is not maximally isotropic because $1 + u$ is a nontrivial common divisor. This is also clear in terms of operators, because all operators Z_x commute with $\mathbf{w}(\xi_1)$, but cannot be obtained by products of translates of $\mathbf{w}(\xi_1)$. ♢

In particular, the greatest common divisor comes into play. We will be able to state more results in the one-dimensional case ($s = 1$), due to the fact that the ring of polynomials $\mathcal{P} := \mathcal{P}_1 = \mathbb{F}[u, u^{-1}]$ is euclidean[6]. Especially this means that the euclidean algorithm can be applied for finding the greatest common

[6]In more abstract words $\mathcal{P}$ is a principal ideal ring, which means that every ideal in $\mathcal{P}$ is generated by a single element. For this general algebraic theory we refer to [Jac75].

divisor of two polynomials, which is also used for the factorization of wavelet transformations [DS98].

Lemma 4.7 (Extended euclidean algorithm for Laurent polynomials) *Let $\xi \in \mathcal{P}^2$ be a phase space vector. Then there exist $f_0, f_1 \in \mathcal{P}$ such that*

$$f_0\xi_+ + f_1\xi_- = \gcd(\xi_+, \xi_-) \tag{4.18}$$

holds.

Proof: We define the degree of a Laurent polynomial $f = \sum_{x=L_-}^{L_+} f_x u^x$ by $\deg(f) := L_+ - L_-$ when f_{L_-} and f_{L_+} are nonzero. Suppose $\deg(\xi_+) \geq \deg(\xi_-)$ and let $r_0 = \xi_+$ and $r_1 = \xi_-$. We make a division with remainder and get a polynomial q_0 with $\deg(q_0) = \deg(r_0) - \deg(r_1)$ and a polynomial r_2 with $\deg(r_2) < \deg(r_1)$ such that

$$r_0 = q_0 r_1 + r_2. \tag{4.19}$$

With this decomposition we get $\gcd(r_0, r_1) = \gcd(r_1, r_2)$. We repeat this division recursively until the remainder vanishes:

$$r_i = q_i r_{i+1} + r_{i+2} \tag{4.20}$$

$$r_{n+1} = q_{n+1} r_n. \tag{4.21}$$

Then we have $r_n = \gcd(r_n, r_{n+1}) = \gcd(r_0, r_1)$. We rewrite the recursion to get the form of Eq. (4.18):

$$\begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{i-2} \end{pmatrix} \begin{pmatrix} r_{i-2} \\ r_{i-1} \end{pmatrix}$$

So we get

$$\begin{pmatrix} r_n \\ 0 \end{pmatrix} = \Gamma_n \dots \Gamma_0 \begin{pmatrix} r_0 \\ r_1 \end{pmatrix}$$

with

$$\Gamma_i := \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix},$$

and since all entries in the matrices are polynomials we get polynomials f_0 and f_1 such that

$$r_n = f_0 r_0 + f_1 r_1$$

holds. ■

4.3 Main Results

4.3.1 Characterization of Clifford Quantum Cellular Automata

We have seen in Proposition 4.4 that symplectic cellular automata are nothing else but linear functions on the phase space $\Xi_s = \mathcal{P}_s^2$ that preserve the $\mathcal{P}_s$-symplectic form $\hat{\sigma}$. Such a map on $\mathcal{P}_s^2$ can be represented by a two-by-two matrix with entries in the polynomial ring $\mathcal{P}_s$. The first column is given by $\mathbf{t}_1 = \mathbf{t}\binom{1}{0}$ ("the local rule for X") and the second column by $\mathbf{t}_2 = \mathbf{t}\binom{0}{1}$ ("the local rule for Z"). The commutation relations of the local rule then end up in the following conditions on the column vectors:

Corollary 4.8 *A two-by-two matrix* $\mathbf{t}$ *with entries in* $\mathcal{P}_s$ *is a symplectic cellular automaton, if and only if, the column vectors of* $\mathbf{t} = (\mathbf{t}_1, \mathbf{t}_2)$ *fulfill* $\hat{\sigma}(\mathbf{t}_1, \mathbf{t}_1) = 0 = \hat{\sigma}(\mathbf{t}_2, \mathbf{t}_2)$ *and* $\hat{\sigma}(\mathbf{t}_1, \mathbf{t}_2) = 1$.

The column vectors $\mathbf{t}_{1,2}$ of a symplectic cellular automaton generate maximally isotropic $\mathcal{P}_s$-subspaces $\mathcal{P}_s\mathbf{t}_{1,2}$, since these are the images of the basis vectors $\binom{1}{0}$ and $\binom{0}{1}$ under the invertible symplectic transformation $\mathbf{t}$. Because the basis vectors generate by construction maximally isotropic subspaces, this must then also be true for the images $\mathbf{t}_{1,2}$.

In the following Subsection, we shall see that the classification of one-dimensional symplectic cellular automata is easier to handle. A useful observation is that a s-dimensional symplectic cellular automaton $\mathbf{t} \in \mathcal{M}_2(\mathcal{P}_s)$ induces for each direction $k = 1, \ldots, s$ a one-dimensional cellular automaton. To see this, we introduce for each direction $k = 1, \ldots, s$ a surjective ring homomorphism $\mathbf{r}_k$ which maps the polynomial ring $\mathcal{P}_s$ of s-variables $u_1, \cdots, u_s, u_1^{-1}, \cdots, u_s^{-1}$ onto the ring $\mathcal{P}$ of one variable u. The ring homomorphism $\mathbf{r}_k$ assigns to a polynomial $f \in \mathcal{P}_s$ the polynomial

$$\mathbf{r}_k f(u) := \sum_{(x^1,\ldots,x^s)\in\mathbb{Z}^s} f(x^1, \ldots, x^s)\ u^{x^k} \tag{4.22}$$

which only depends on the variables u, u^{-1}. The ring homomorphism $\mathbf{r}_k$ evaluates the polynomial $f \in \mathcal{P}_s$ at $u_l = 1$, for $l \neq k$, whereas $u_k = u$ is the remaining free variable.

For a symplectic cellular automaton $\mathbf{t} \in \mathcal{M}_2(\mathcal{P}_s)$ the conditions $\hat{\sigma}(\mathbf{t}_{1,2}, \mathbf{t}_{1,2}) = 0$ and $\hat{\sigma}(\mathbf{t}_1, \mathbf{t}_2) = 1$ are identities of polynomials. The matrix $\mathbf{r}_k\mathbf{t} \in \mathcal{M}_2(\mathcal{P})$ is build by applying the ring homomorphism $\mathbf{r}_k$ to each matrix element individually. Obviously, the identities $\mathbf{r}_k\hat{\sigma}(\mathbf{t}_{1,2}, \mathbf{t}_{1,2}) = \hat{\sigma}(\mathbf{r}_k\mathbf{t}_{1,2}, \mathbf{r}_k\mathbf{t}_{1,2}) = 0$ as well as $\mathbf{r}_k\hat{\sigma}(\mathbf{t}_1, \mathbf{t}_2) = \hat{\sigma}(\mathbf{r}_k\mathbf{t}_1, \mathbf{r}_k\mathbf{t}_2) = 1$ follow. As a consequence we get:

Corollary 4.9 *Let $\mathbf{t} \in \mathcal{M}_2(\mathcal{P}_s)$ be a s-dimensional symplectic cellular automaton. Then for each direction $k = 1, \ldots, s$, the two-by-two matrix $\mathbf{r}_k\mathbf{t} \in \mathcal{M}_2(\mathcal{P})$ is a one-dimensional symplectic cellular automaton.*

Now it is easy to show that symplectic cellular automata are reflection invariant and that the determinant is a monomial. It is slightly more involved that we have reflection invariance with respect to a lattice point and not with respect to an half integer lattice point.

Theorem 4.10 *A $\mathcal{P}_s$-linear map $\mathbf{t} \in \mathcal{M}_2(\mathcal{P}_s)$ is a symplectic cellular automaton, if and only if, the following holds:*

1. *The matrix $\mathbf{t}$ is reflection invariant with respect to some lattice point $a \in \mathbb{Z}^s$.*
2. *The $\mathcal{P}_s$-valued determinant of $\mathbf{t}$ is $\det(\mathbf{t}) = u^{2a}$.*

Proof: If $\mathbf{t}$ is a symplectic cellular automaton, then the column vectors $\mathbf{t}_{1,2}$ generate maximally isotropic subspaces. By Lemma 4.5 it follows that $\mathbf{t}_1$, respectively $\mathbf{t}_2$, is reflection invariant to some half integer lattice point a, respectively b. Since $\mathbf{t}$ preserves the symplectic form $\hat{\sigma}$ we obtain $1 = \hat{\sigma}(\mathbf{t}_1, \mathbf{t}_2) = \hat{\sigma}(u^{2a}\overline{\mathbf{t}_1}, u^{2b}\overline{\mathbf{t}_2}) = u^{2(b-a)}\hat{\sigma}(\overline{\mathbf{t}_1}, \overline{\mathbf{t}_2}) = u^{2(b-a)}$ and therefore $a = b$ for an half-integer lattice point $a \in \frac{1}{2}\mathbb{Z}^s$. As a consequence, $\mathbf{t}$ is reflection invariant for $a \in \frac{1}{2}\mathbb{Z}^s$. Now, $1 = \hat{\sigma}(\mathbf{t}_1, \mathbf{t}_2) = \hat{\sigma}(u^{2a}\overline{\mathbf{t}_1}, \mathbf{t}_2) = u^{-2a}\det(\mathbf{t}_1, \mathbf{t}_2)$.

Vice versa, let $\mathbf{t}$ be a matrix, which is invariant with respect to the reflection at a and whose determinant is $\det(\mathbf{t}) = u^{2a}$. Then the column vectors $\mathbf{t}_{1,2}$ are reflection invariant, which implies (by Lemma 4.5) that $\hat{\sigma}(\mathbf{t}_{1,2}, \mathbf{t}_{1,2}) = 0$ holds. The determinant of $\mathbf{t}$ is u^{2a} which implies $\hat{\sigma}(\mathbf{t}_1, \mathbf{t}_2) = 1$. Thus $\mathbf{t}$ preserves the symplectic form $\hat{\sigma}$.

By Corollary 4.9, we obtain a one-dimensional symplectic cellular automaton $\mathbf{r}_k\mathbf{t}$ for each lattice direction $k = 1, \ldots, s$. We have already shown that the column vectors $\mathbf{t}_{1,2}$ are reflection invariant for $a = (a^1, \ldots, a^s)$, which implies that for each direction k the column vectors $\mathbf{r}_k\mathbf{t}_{1,2}$ are reflection invariant for a^k. We also have that $\mathbf{r}_k\mathbf{t}_{1,2}$ generate maximally isotropic $\mathcal{P}$-subspaces, since these define valid cellular automaton rules.

Suppose now, that $f \in \mathcal{P}$ is reflection invariant for $b \in \frac{1}{2}\mathbb{Z}$ in the half-integer lattice. Then we can translate f by an even translation $2y \in 2\mathbb{Z}$, such that $c = 2(b + y)$ is either 0 or 1. If f is of even length, then $c = 1$ follows. The polynomial $u^y f$ is reflection invariant for $1/2$ and can be expanded as

$$u^y f = \sum_{n \in \mathbb{N}} c_n \left(u^{n+1} + u^{-n}\right). \tag{4.23}$$

Now, for each $n \in \mathbb{N}$, the polynomial $u^{n+1} + u^{-n}$ is a multiple of $u + 1$. Thus f is also a multiple[7] of $u^{-y}(u + 1)$. From this we conclude that, if b is not an

[7]Note that the coefficients are from the finite field $\mathbb{Z}_p$.

integer, then a reflection invariant $\xi \in \mathcal{P}^2$ is a multiple of $u^{-y}(u+1)$ and does not generate a maximally isotropic $\mathcal{P}$-subspace, since $u+1$ is a nontrivial common divisor of ξ_+ and ξ_-, which is a contradiction. So a^k must be an integer lattice point, that is, $a = (a^1, \ldots, a^s) \in \mathbb{Z}^s$. ■

So each symplectic cellular automaton $\mathbf{t}$ is reflection invariant for the reflection at some lattice point $a \in \mathbb{Z}^s$. Therefore, the symplectic cellular automaton $u^{-a}\mathbf{t}$ is reflection invariant with respect to the origin $x = 0$. In the subsequent, we call all symplectic cellular automata, which are reflection invariant with respect to the origin, to be "centered" and it is sufficient to classify only those. The polynomials in $\mathcal{P}_s$ which are reflection invariant with respect to the origin form a subring $\mathcal{R}_s \subset \mathcal{P}_s$ and will be simply called reflection invariant (for $s = 1$ we will again omit the index). From Theorem 4.10, we obtain a handy characterization of centered symplectic cellular automata:

Corollary 4.11 *The group of centered symplectic cellular automata is given by the group* $\mathrm{SL}(2, \mathcal{R}_s)$ *of two-by-two matrices* $\mathbf{t}$ *with entries in the subring* $\mathcal{R}_s$ *of reflection invariant polynomials and* $\mathcal{R}_s$*-valued determinant* $\det(\mathbf{t}) = 1$.

Example 4.12 The symplectic transformation corresponding to the "cluster state QCA" from Eq. (4.1) is given by

$$\mathbf{t} = \begin{pmatrix} 0 & 1 \\ 1 & u + u^{-1} \end{pmatrix} . \tag{4.24}$$

Obviously all entries are reflection invariant with respect to the origin and the determinant is equal to one (modulo 2). ◊

A nice aspect of Corollary 4.11 is that the centered symplectic cellular automata can be obtained by the following strategy: Choose two arbitrary reflection invariant $f, h \in \mathcal{R}_s$ and find all possible factorizations of the polynomial $fh - 1 = f'h'$ into a product of two reflection invariant $f', h' \in \mathcal{R}_s$. The corresponding symplectic cellular automaton is then given by

$$\begin{pmatrix} f & f' \\ h' & h \end{pmatrix} \in \mathrm{SL}(2, \mathcal{R}_s) . \tag{4.25}$$

Even if the task of factorizing the polynomial $fh - 1$ is quite cumbersome, there is always a "trivial" solution, namely, $h' = 1$ and $f' = fh - 1$. The matrix

$$\begin{pmatrix} f & fh - 1 \\ 1 & h \end{pmatrix} \in \mathrm{SL}(2, \mathcal{R}_s) \tag{4.26}$$

describes the corresponding symplectic cellular automaton.

Another remarkable fact is that, due to Cramer's rule, the inverse of a centered symplectic CA $\mathbf{t}$ is simply given by

$$\mathbf{t}^{-1} = \begin{pmatrix} \mathbf{t}_{22} & -\mathbf{t}_{12} \\ -\mathbf{t}_{21} & \mathbf{t}_{11} \end{pmatrix} . \tag{4.27}$$

Similarly we have that for a symplectic CA $\mathbf{t}$ containing a translation by a positions, i.e. $\det(\mathbf{t}) = u^{2a}$, the inverse contains a translation by $-a$ positions.

Since every Clifford QCA is up to a global shift centered, the index is just given by the shift component (compare Chapter 3). In particular, when we have $\det \mathbf{t} = u^{2a}$ for the symplectic cellular automaton, then it is clear that the index of the corresponding QCA T is given by

$$\mathrm{ind}(T) = p^a . \tag{4.28}$$

4.3.2 1D CQCAs and Translationally Invariant Stabilizer States

In this Subsection we are investigating one-dimensional symplectic cellular automata. As already mentioned, we can achieve more results in this case, because we can apply the euclidean algorithm (Lemma 4.7). We will use the euclidean algorithm to show that for every reflection invariant $\xi \in \mathcal{P}^2$ with $\gcd(\xi_+, \xi_-) = 1$, there exists at least one corresponding reflection invariant η such that $\hat{\sigma}(\eta, \xi) = 1$ holds and is therefore a valid column of a symplectic cellular automaton matrix. We will use this fact to show that every uniquely determined and translationally invariant stabilizer state can be prepared from a product state by applying one timestep of a Clifford QCA.

Stabilizer states are studied extensively in the last years ([Got97] and [NC00] are just examples, which are useful as introductory texts). The basic concept is to fix an abelian group of operators (usually a subgroup of the Pauli group), also called stabilizer group, and to define a stabilizer state as common eigenvector of all these operators. In our case we are looking for translationally invariant states, so the stabilizer group is generated by all translates of one single Weyl operator $\mathbf{w}(\xi)$ for some phase space vector $\xi \in \mathcal{P}^2$. The state should fulfill $\omega(\tau^x \mathbf{w}(\xi)) = \omega(\mathbf{w}(\alpha^x \xi)) = 1$ for all $x \in \mathbb{Z}$. The stabilizer formalism is often studied for finitely many qudits. In that case it is known that the stabilizer state is uniquely determined, if the number of generating operators is large enough (see e.g. [NC00] for a quantitative statement). In our situation we have infinitely many qudits, so we cannot apply this result. But it turns out that the operators $\mathbf{w}(\alpha^x \xi)$ must generate a maximal abelian algebra, or equivalently, the subspace $\mathcal{P}\xi$ must be maximally isotropic.

Theorem 4.13 *For a phase space vector $\xi \in \mathcal{P}^2$ the following is equivalent:*

1. *There exists a uniquely determined state* ω *with* $\omega(\mathbf{w}(\alpha^x\xi)) = 1$ *for all* $x \in \mathbb{Z}$.

2. $\mathcal{P}\xi$ *is a maximally isotropic* $\mathcal{P}$*-subspace.*

3. *There is a Clifford QCA* T *with* $\mathbf{w}(\xi) = T(\mathbf{w}(0,1))$.

4. ξ *is reflection invariant and* $\gcd(\xi_+, \xi_-) = 1$.

For the proof of this Theorem we need that a singly generated isotropic subspace can always be embedded into a singly generated maximally isotropic subspace:

Lemma 4.14 *Let* $0 \neq \xi \in \mathcal{P}_s^2$ *and* $\mathcal{P}_s\xi$ *be an isotropic, but not maximally isotropic* $\mathcal{P}_s$*-subspace. Then there exists a phase space vector* $\eta \in \mathcal{P}_s^2$ *such that* $\mathcal{P}_s\eta \supsetneq \mathcal{P}_s\xi$ *is maximally isotropic.*

Proof: $\mathcal{P}_s\xi$ is isotropic if and only if the equation $0 = \hat{\sigma}(\xi,\xi) = \overline{\xi}_+\xi_- - \overline{\xi}_-\xi_+$ holds. We make a distinction of cases for this equation:

i. $\xi_+ = 0$ (analogously $\xi_- = 0$): Then $\mathcal{P}_s\xi = \{0\} \oplus \mathcal{P}_s\xi_-$ and ξ_- is not invertible since this would force $\mathcal{P}_s\xi = \{0\} \oplus \mathcal{P}_s$ to be maximally isotropic. So we can set $\eta = (0,1)$.

ii. $\xi_+ = f\xi_-$ (analogously $\xi_- = f\xi_+$) with f reflection invariant: Then we have $\mathcal{P}_s\xi = \mathcal{P}_s\xi_-(f,1)$. We set $\eta = (f,1)$ and get that $\mathcal{P}_s\eta$ is a maximally isotropic subspace since $0 = \hat{\sigma}(\eta,\lambda) = f\lambda_- - \lambda_+$ implies $\lambda = \lambda_-\eta \in \mathcal{P}_s\eta$.

iii. $\xi_+ \neq 0 \neq \xi_-$ and $\xi_\pm \neq f\xi_\mp$: Then $\xi = f\overline{\xi}$ with f invertible, so ξ is reflection invariant for some $n \in \frac{1}{2}\mathbb{Z}^d$. Because $\mathcal{P}_s\xi$ is not maximally isotropic we can find $\eta \notin \mathcal{P}_s\xi$ with $0 = \hat{\sigma}(\xi,\eta) = u^n(\xi_+\eta_- - \xi_-\eta_+)$. Since ξ_+ and ξ_- are nonvanishing this implies $\xi = g\eta$ for some $g \in \mathcal{P}_s$. We can choose $\gcd(\eta_+,\eta_-) = 1$ and $\mathcal{P}_s\eta$ to be maximally isotropic.

■

Proof of Theorem 4.13: 2. $\Longrightarrow$ 4. Because $\mathcal{P}\xi$ is a maximally isotropic subspace we conclude from Lemma 4.5 that ξ is reflection invariant with $\gcd(\xi_+,\xi_-) = 1$.

4. $\Longrightarrow$ 3. We have to find $\eta \in \mathcal{P}^2$ with $\hat{\sigma}(\eta,\xi) = 1$ and $\hat{\sigma}(\eta,\eta) = 0$. With Lemma 4.7 we find a solution $f_\pm \in \mathcal{P}$ of the equation $f_+\xi_+ + f_-\xi_- = \gcd(\xi_+,\xi_-) = 1$ and $\eta' := (\overline{f}_-, -\overline{f}_+)$ is a solution of $\hat{\sigma}(\eta',\xi) = 1$. Yet we do not know, whether η' is reflection invariant, or equivalently, whether $\hat{\sigma}(\eta',\eta') = 0$ holds. But if η' is a solution of $\hat{\sigma}(\eta',\xi) = 1$ then the same is true for $\eta = \eta' + f\xi$. Thus we have to solve the condition $0 = \hat{\sigma}(\eta,\eta) = \hat{\sigma}(\eta',\eta') + \hat{\sigma}(f\xi,\eta') + \hat{\sigma}(\eta',f\xi) = \hat{\sigma}(\eta',\eta') - \overline{f} + f$. The polynomial $h := \hat{\sigma}(\eta',\eta')$ is anti-symmetric with respect to the reflection

$\xi \mapsto \overline{\xi}$ and it can be expanded as $h = \sum_{n>0} h_n(u^n - u^{-n})$. By choosing $f = \sum_{n>0} h_n u^n$ we find that $\eta = \eta' + f\xi$ is indeed reflection invariant. The matrix $(\xi, \eta) \in \mathrm{SL}(2, \mathcal{R})$ is then a symplectic cellular automaton and induces a Clifford QCA with the desired property.

3. $\Longrightarrow$ 1. Consider a state ω with the desired property. Then this state is equal to $\tilde{\omega} \circ T$, where $\tilde{\omega}$ is a state with $\tilde{\omega}(\tau^x \mathbf{w}(0,1)) = 1$ for all $x \in \mathbb{Z}$, so the stabilizer group of this state is given by all translates of $\mathbf{w}(0,1)$. This means $\tilde{\omega}$ is a translationally invariant product state, which is determined by the equation $\tilde{\omega}(\mathbf{w}(0,1)) = 1$ and corresponds to the one dimensional projector onto the eigenspace of $\mathbf{w}(0,1)$ with eigenvalue 1. Therefore this state is uniquely determined and $\omega = \tilde{\omega} \circ T$ is the unique state with $\omega(\mathbf{w}(\alpha^x \xi)) = 1$.

1. $\Longrightarrow$ 2. Suppose $\mathcal{P}\xi$ is an isotropic $\mathcal{P}$-subspace but not maximally isotropic. By Lemma 4.14, we know that there exists a phase space vector ξ' with $\mathcal{P}\xi \subsetneqq \mathcal{P}\xi'$. So we have $\xi = f\xi'$ with f not invertible and Lemma 4.5 tells us that ξ' is reflection invariant. With help of the euclidean algorithm we find a QCA T and a corresponding symplectic transformation $\mathbf{t}$ with $T(\mathbf{w}(0,1)) = \mathbf{w}(\mathbf{t}(0,1)) = \mathbf{w}(\xi')$ (just as step two of this proof). Now consider a product state φ with $\varphi(\mathbf{w}(0,u^x)) = \exp(\frac{2\pi i}{p} a_x)$ depending on the a_x. We transform this state with T^{-1} and the expectation values of the operators $\tau^x \mathbf{w}(\xi)$ should be all equal to 1:

$$\begin{aligned}
1 &= \varphi_{T^{-1}}(\tau^x \mathbf{w}(\xi)) = \varphi(\tau^x \mathbf{w}(\mathbf{t}^{-1}\xi)) \\
&= \varphi(\tau^x \mathbf{w}(\mathbf{t}^{-1}(f\xi'))) = \varphi(\tau^x \mathbf{w}(\hat{f} \star \widehat{(0,1)})) \\
&= \varphi\Big(\mathbf{w}(\sum_k \hat{f}_{-k} \delta_{k+x}(0,1))\Big) = \prod_k \hat{f}_{-k} \varphi(\mathbf{w}(\delta_{k+x}(0,1))) \\
&= \exp\Big(\frac{2\pi i}{p} \sum_k \hat{f}_{-k} a_{k+x}\Big)
\end{aligned}$$

So we have to solve the equations $\sum_k \hat{f}_{-k} a_{k+x} = 0$ to get appropriate a_x and therefore states with the desired property. Since f is not invertible the support of $\hat{f}$ is not a one-elementary set. Let $I = \{-L_-, \ldots, -L_+\}$ be the minimal interval such that $\mathrm{supp}(\hat{f}) \subset I$. We can choose arbitrary $a_{L_-}, \ldots, a_{L_+-1}$ to compute a_{L_+} from the equation $\sum_k \hat{f}_{-k} a_k$. Recursively all a_x can be calculated from the other equations but the solution will depend from the initial choice of the $a_{L_-}, \ldots, a_{L_+-1}$. This means that there exists more than one state φ of the above form, such that $1 = \varphi_{T^{-1}}(\tau^x \mathbf{w}(\xi))$ is fulfilled. So the uniqueness of the state in 1. forces $\mathcal{P}\xi$ to be maximally isotropic. ■

So we have shown that every translationally invariant and uniquely determined stabilizer state in a one-dimensional lattice can be prepared out of a product state by a single timestep of a Clifford QCA. Unfortunately we cannot generalize this result to higher lattice dimensions, because Lemma 4.7 is only valid for univariate polynomials. The euclidean algorithm for computing the greatest

common divisor can be generalized to multivariate polynomials [Bro74], but the extended version (equation (4.18)) does not hold.

Example 4.15 We consider again the phase space vectors $\xi_1 = (1+u)\binom{0}{1}$ and $\xi_2 = \binom{1}{u+u^{-1}}$ (see Example 4.6). As already mentioned, the phase space vector ξ_1 is reflection invariant for 1/2 and generates an isotropic $\mathcal{P}$-subspace, but none of the statements of Theorem 4.13 holds: The expectation value of $\mathbf{w}(\alpha^x\xi_1) = Z_x \otimes Z_{x+1}$ is equal to one both in the "all spins up" and in the "all spins down" state, so there is no uniquely determined stabilizer state. As we have seen in 4.6 the subspace $\mathcal{P}\xi_1$ is not maximally isotropic. The reflection invariance does not hold for an integer lattice point, so ξ_1 is not a valid column of a symplectic CA, and $1+u$ is a common divisor of $\xi_{1,+}$ and $\xi_{1,-}$, which is not invertible.

In contrast ξ_2 fulfills all four conditions. The uniquely determined stabilizer state is given by the one-dimensional cluster state and a possible CQCA is given by Example 4.1. ◊

4.3.3 Factorization of 1D Clifford QCAs

We have seen that the set of centered CQCAs forms a group and that this group is given by 2×2-matrices with determinant one and reflection invariant polynomials as matrix elements. In the one-dimensional case the group structure can be more clarified, since we are able to give a complete set of generators, which can be regarded as elementary operations.

A simple example of a 2×2-matrix in $\mathrm{SL}(2,\mathcal{R})$ is for some reflection invariant polynomial $f \in \mathcal{R}$ given by

$$\mathbf{g}(f) := \begin{pmatrix} 1 & 0 \\ f & 1 \end{pmatrix}, \tag{4.29}$$

which we will call "shear transformation". In particular, $\mathbf{g}(f_1+f_2) = \mathbf{g}(f_1)\mathbf{g}(f_2)$ holds[8] for all $f_1, f_2 \in \mathcal{R}$. The symmetric polynomials $w_n = u^n + u^{-n}$, $n \in \mathbb{N}$, and $w_0 = 1$ form a basis of the subring $\mathcal{R}$. Thus every shear transformation can be decomposed into a finite product of elementary shear transformations $\mathbf{g}(cw_n)$ with $n \in \mathbb{N}\cup\{0\}$ and $c \in \mathbb{F}$.

The local rule of the corresponding QCA G_n with $G_n\mathbf{w}(\xi) = \mathbf{w}(\mathbf{g}(w_n)\xi)$ is for $n \geq 1$ given by

$$\begin{array}{lcl} G_n(X_0) & = & Z_{-n}\otimes \quad \otimes\cdots\otimes \quad X_0 \quad \otimes \quad \otimes\cdots\otimes Z_n \\ G_n(Z_0) & = & \qquad\qquad\qquad\quad Z_0 \end{array} . \tag{4.30}$$

For $n = 0$ we have the single cell operation ("local shear transformation")

$$\begin{array}{lcl} G_0(X_0) & = & \mathbf{w}(1,1) \\ G_0(Z_0) & = & \quad Z_0 \end{array} , \tag{4.31}$$

[8] This means, the map $f \mapsto \mathbf{g}(f)$ is a group homomorphism from the additive group $\mathcal{R}$ into the group of centered symplectic cellular automata $\mathrm{SL}(2,\mathcal{R})$.

which correspond for $p = 2$ to applying the phase gate $\begin{pmatrix} 1 & \\ & i \end{pmatrix}$ to all single cells.

Another single cell operation is the "local Fourier transformation", which is in phase space given by the matrix

$$\mathbf{f}_c = \begin{pmatrix} 0 & -c \\ 1/c & 0 \end{pmatrix} \tag{4.32}$$

with some constant $0 \neq c \in \mathbb{F}$ (for $c = 1$ we will write $\mathbf{f} := \mathbf{f}_1$). For $p = 2$ we have $c = 1$ and the corresponding QCA switches the operators X and Z in each single cell and is therefore given by applying the Hadamard matrix.

Note that all symplectic single cell transformations can be obtained by a product of local shear and local Fourier transformations, which is a generalization to higher cell dimensions of the fact that local Clifford operations are generated by Hadamard and phase gate.

The symplectic transformations $\mathbf{g}(f), \mathbf{f}_c$ are elementary symplectic cellular automata in the sense of the following theorem.

Theorem 4.16 *The group of centered symplectic cellular automata* $\mathrm{SL}(2, \mathcal{R})$ *is generated by the set* $\{\mathbf{g}(w_n) | n \in \mathbb{N} \cup \{0\}\} \cup \{\mathbf{f}_c | c \in \mathbb{F}\}$.

For the proof of this Theorem we need the following notations: Given a polynomial $f \in \mathcal{P}$ the coefficient of the monomial u^x is $\langle f \rangle_x$. Recall that "degree" of a polynomial in $f \in \mathcal{P}$ is defined by $\deg(f) := \max\{x | \langle f \rangle_x \neq 0\} - \min\{x | \langle f \rangle_x \neq 0\}$ and that the support is defined by $\mathrm{supp}(f) := \{x | \langle f \rangle_x \neq 0\}$.

Lemma 4.17 *Let* (ξ, η) *be a symplectic cellular automaton which is invariant under the reflection at the origin:* $\xi = \overline{\xi}$ *and* $\eta = \overline{\eta}$. *If the degrees of column vectors fulfill* $\deg(\xi) > \deg(\eta)$ *then there exists a shear transformation* $\mathbf{g}(f)$, *with reflection invariant* $f \in \mathcal{P}$, *such that the symplectic transformation*

$$(\xi', \eta') = (\xi, \eta)\mathbf{g}(f)\mathbf{f}_1 \tag{4.33}$$

satisfies $\deg(\xi, \eta) > \deg(\xi', \eta')$ *and* $\deg(\xi') > \deg(\eta')$.

Proof: Since ξ and η are reflection invariant, the degree is an even integer and we introduce $x := \deg(\xi)/2$, $y := \deg(\eta)/2$, as well as $n_1 := x - y > 0$. We conclude from the identity $\hat{\sigma}(\xi, \eta) = 1$ that

$$\langle \hat{\sigma}(\xi, \eta) \rangle_{x+y} = \langle \xi_+ \rangle_{-x} \langle \eta_- \rangle_y - \langle \xi_- \rangle_{-x} \langle \eta_+ \rangle_y = 0 \tag{4.34}$$

is valid. This implies that

$$\langle \xi \rangle_x = \langle \xi \rangle_{-x} = -f_1 \langle \eta \rangle_y = -f_1 \langle \eta \rangle_{-y} \tag{4.35}$$

for some $f_1 \in \mathbb{F}$. Now $\langle \xi + f_1(u^{n_1} + u^{-n_1})\eta \rangle_{\pm x} = 0$ which implies that

$$\deg(\xi + f_1(u^{n_1} + u^{-n_1})\eta) < \deg(\xi) \; . \tag{4.36}$$

Now we observe

$$\begin{aligned} (\xi_1, \eta_1) &:= (\xi, \eta)\mathbf{g}(f_1(u^{n_1} + u^{-n_1})) \\ &= \begin{pmatrix} \xi_+ & \eta_+ \\ \xi_- & \eta_- \end{pmatrix} \begin{pmatrix} 1 & 0 \\ f_1(u^{n_1} + u^{-n_1}) & 1 \end{pmatrix} \\ &= \begin{pmatrix} \xi_+ + f_1(u^{n_1} + u^{-n_1})\eta_+ & \eta_+ \\ \xi_- + f_1(u^{n_1} + u^{-n_1})\eta_- & \eta_- \end{pmatrix} \end{aligned} \tag{4.37}$$

from which we conclude that $\deg(\xi_1, \eta_1) < \deg(\xi, \eta)$. If $\deg(\xi_1) > \deg(\eta_1)$ we can find a shear transformation $\mathbf{g}(f_2(u^{n_2} + u^{-n_2}))$ such that

$$(\xi_2, \eta_2) = (\xi_1, \eta_1)\mathbf{g}(f_2(u^{n_2} + u^{-n_2})) \tag{4.38}$$

fulfills $\deg(\xi_2, \eta_2) < \deg(\xi_1, \eta_1)$. We can proceed this reduction until the lth step with $2l = |\mathrm{supp}(\xi) \setminus \mathrm{supp}(\eta)|$. The resulting symplectic cellular automaton

$$(\xi_l, \eta_l) = (\xi_{l-1}, \eta_{l-1})\mathbf{g}(f_l(u^{n_l} + u^{-n_l})) \tag{4.39}$$

then satisfies $\deg(\xi_l) \leq \deg(\eta_l)$. If $\deg(\xi_l) = \deg(\eta_l)$ then, there is an appropriate constant $f_{l+1} \in \mathbb{F}$ such that

$$(\xi', \eta') = (\xi, \eta)\mathbf{g}(f)\mathbf{f}_1 = (-\eta_l, \xi_l + f_{l+1}\eta_l) \tag{4.40}$$

holds with $\deg(\xi') > \deg(\eta')$. Here f is the reflection invariant polynomial

$$f = \sum_{j=1}^{l+1} f_j(u^{n_j} + u^{-n_j}) \; . \tag{4.41}$$

If $\deg(\xi_l) < \deg(\eta_l)$, then the shear transformation $\mathbf{g}(f_{l+1})$ is not applied and we get

$$(\xi', \eta') = (\xi, \eta)\mathbf{g}(f)\mathbf{f}_1 = (-\eta_l, \xi_l) \tag{4.42}$$

with the polynomial $f = \sum_{j=1}^{l} f_j(u^{n_j} + u^{-n_j})$. ■

Proof of Theorem 4.16: Let (ξ_0, η_0) be a symplectic cellular automaton which is invariant under the reflection at the origin. Then, by Lemma 4.17, there exists a symplectic cellular automaton (ξ_1, η_1) and a shear transformation $\mathbf{g}(f_1)$ such that

$$(\xi_0, \eta_0) = (\xi_1, \eta_1)\mathbf{g}(f_1)\mathbf{f}_1 \tag{4.43}$$

and $\deg(\xi_1) > \deg(\eta_1)$. Thus we can iterate this reduction process until (ξ_k, η_k) is a constant symplectic transformation (corresponding to a QCA with single cell neighborhood), which can be decomposed into a product of local shear transformations $\mathbf{g}(w_0)$ and local Fourier transforms $\mathbf{f}_{c_i}$ with $c_i \in \mathbb{F}$. This yields the following decomposition of (ξ_0, η_0):

$$(\xi_0, \eta_0) = \mathbf{g}(f_r)\mathbf{f}_{c_r} \cdots \mathbf{g}(f_2)\mathbf{f}_{c_2}\mathbf{g}(f_1)\mathbf{f}_{c_1} \ . \tag{4.44}$$

■

A more concrete formulation of the statement of Theorem 4.16 is that every one-dimensional centered symplectic cellular automaton $\mathbf{t}$ is a finite product of shear transformations and local fourier transforms of the following form:

$$\mathbf{t} = \mathbf{g}(f_r)\mathbf{f}_{c_r} \cdots \mathbf{g}(f_2)\mathbf{f}_{c_2}\mathbf{g}(f_1)\mathbf{f}_{c_1} \tag{4.45}$$

with reflection invariant polynomials $f_1, \ldots, f_r \in \mathcal{R}$ and constants $c_1, \ldots, c_r \in \mathbb{F}$.

Example 4.18 Let us consider in the qubit case ($p = 2$) the symplectic cellular automaton

$$\mathbf{t} = \begin{pmatrix} w_1 & 1 \\ 1 + w_2 & w_1 \end{pmatrix} \tag{4.46}$$

and, since $w_2 = {w_1}^2$ for $p = 2$, we have $\det(\mathbf{t}) = 1$. The corresponding CQCA is given by

$$\begin{array}{rcccccc} T(X_0) & = & Z_{-2} \otimes X_{-1} \otimes & Z_0 & \otimes X_1 \otimes Z_2 \\ T(Z_0) & = & Z_{-1} \otimes & X_0 & \otimes Z_1 \end{array} \ . \tag{4.47}$$

The basic idea for deriving a decomposition like (4.45) is to reduce the support of the first column of $\mathbf{t}$ by applying a shear transformation from the right. We get

$$\mathbf{t}\mathbf{g}(w_1) = \begin{pmatrix} 0 & 1 \\ 1 & w_1 \end{pmatrix} \ . \tag{4.48}$$

This matrix is obviously equal to $\mathbf{g}(w_1)\mathbf{f}$ and we have

$$\mathbf{t} = \mathbf{g}(w_1)\mathbf{f}_c\mathbf{g}(w_1) \ , \tag{4.49}$$

which is indeed a decomposition in accordance with (4.45). ◊

For $p = 2$ all the generators $\mathbf{g}(f)$ and $\mathbf{f}$ are their own inverses, so the time evolution of these operations alternates between the identity and a single timestep of the automaton. Especially these QCAs show no propagation, because the neighborhood of the iterated automaton does not increase with the number of timesteps. A nontrivial time evolution only occurs, if the symplectic cellular automaton is composed of at least two different generators.

4.4 Periodic Boundary Conditions

In this Chapter we are looking for translationally invariant Clifford operations with periodic boundary conditions on a s-dimensional lattice. These boundary conditions are given by a s-dimensional torus $\mathbb{T}^s_N$, which is determined by s independent lattice vectors $N = (N_1, \ldots, N_s)$ (see figure 4.1), and all lattice points which differ by these vectors are identified. The number of (not identified) lattice points is given by $|\mathbb{T}^s_N| := |\det(N_1, \ldots, N_s)|$. We denote here by $\mathcal{P}_{s,N}$ the ring of polynomials $f = \sum_{x \in \mathbb{T}^s_N} f(x)u^x$ such that the u-variables fulfill the periodic boundary conditions $u^{N_1} = u^{N_2} = \ldots = u^{N_s} = 1$. This guaranties that the product of two polynomials from $\mathcal{P}_{s,N}$ is again an element from $\mathcal{P}_{s,N}$. But algebraically there are large differences between $\mathcal{P}_s$ and $\mathcal{P}_{s,N}$: $\mathcal{P}_{s,N}$ is not a division ring, because there are zero divisors and there are in general other invertible elements than $u^x = u_1^{x_1} u_2^{x_2} \cdots u_s^{x_s}$. The reflection $\overline{f}$ is again given by replacing u by u^{-1} or in other words we substitute u^x by u^{N-x}. The symplectic form $\hat{\sigma}$ is then of the same form as in the infinite lattice case.

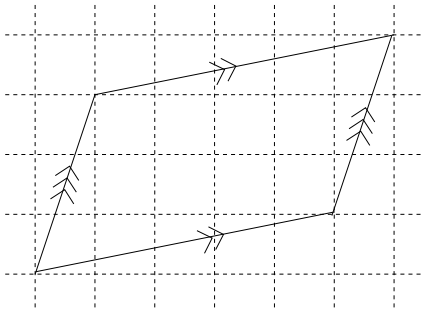

Figure 4.1: *A 2-dimensional torus defined by* $N_1 = (1, 3)$ *and* $N_2 = (5, 1)$.

Now we have to say, how a Clifford QCA (or a symplectic cellular automaton) is defined on these systems. In the general theory of QCAs (see the Wrapping Lemma 2.9), the neighborhood of a QCA with periodic boundary conditions is not allowed to be too large in comparison with the torus. This guaranties that the QCA can be extended to the whole lattice. Since this case is covered by restricting the existing Clifford QCAs to periodic boundary conditions, we drop all locality conditions, and we take the same structure as in Corollary 4.8 as definition of a symplectic cellular automaton:

Definition 4.19 A 2×2 matrix $\mathbf{t} = (\mathbf{t}_1, \mathbf{t}_2)$ with entries in $\mathcal{P}_{s,N}$ is a symplectic cellular automaton if the column vectors fulfill $\hat{\sigma}(\mathbf{t}_1, \mathbf{t}_1) = 0 = \hat{\sigma}(\mathbf{t}_2, \mathbf{t}_2)$ and $\hat{\sigma}(\mathbf{t}_1, \mathbf{t}_2) = 1$.

With this definition it is possible to state an analogous version of Theorem 4.13 also for periodic boundary conditions. But the proof is quite different from the infinite lattice case.

Theorem 4.20 *For a phase space vector $\xi \in \mathcal{P}_{s,N}^2$ the following is equivalent:*

1. *There exists a uniquely determined state ω with $\omega(\mathbf{w}(\alpha^x\xi)) = 1$ for all $x \in \mathbb{T}_N^s$.*

2. *$\mathcal{P}_{s,N}\xi$ is a maximally isotropic $\mathcal{P}_{s,N}$-subspace.*

3. *There is a symplectic cellular automaton $\mathbf{t}$ with $\xi = \mathbf{t}\binom{0}{1}$.*

Proof: 1. $\iff$ 2. A stabilizer state on M qudits is uniquely determined, if and only if, the minimal number of generators of the stabilizer group equals M [NC00, Sch04]. Here we have the $|\,\mathbb{T}_N^s|$ generators $\mathbf{w}(\alpha^x\xi)$. These are independent, if and only if, they generate a maximally abelian algebra, or equivalently, if $\mathcal{P}_{s,N}\xi$ is a maximally isotropic subspace.

2. $\implies$ 3. Since we have a finite dimensional space, there exists a symplectic basis, and any basis of a maximally isotropic subspace can be extended to a symplectic basis [MS98]. For this construction we turn to the original phase space (by inverse "Fourier transform") and define by $\xi_x := \alpha^x\hat{\xi}$ basis vectors of a subspace. Since we know by 2. that this space is isotropic, these vectors fulfill $\sigma(\xi_x, \xi_y) = 0$ and therefore $0 = \tilde{\sigma}(\hat{\xi}, \hat{\xi}) = \hat{\sigma}(\xi, \xi)$. Then there exists a dual vector $\hat{\eta}$ with $\sigma(\hat{\eta}, \xi_x) = \delta_{x0}$ and we define $\eta_y = \alpha^y\hat{\eta}$. We get that $\sigma(\eta_y, \xi_x) = \sigma(\hat{\eta}, \xi_{x-y}) = \delta_{xy}$ holds and so we have $\hat{\sigma}(\eta, \xi) = 1$. We have to verify that we can choose η, such that $\hat{\sigma}(\eta, \eta) = 0$ holds. But if η is a solution to $\hat{\sigma}(\eta, \xi) = 1$ the same is true for $\eta' = \eta + f\xi$ for any $f \in \mathcal{P}_{s,N}$ and we can find similar to the case of Theorem 4.13 an appropriate f with $\hat{\sigma}(\eta', \eta') = 0$.

3. $\implies$ 2. Suppose that $\mathbf{t}$ is a symplectic cellular automaton with $\xi = \mathbf{t}\binom{0}{1}$. Then $\mathbf{t}$ induces a homomorphism between the maximally isotropic subspace $\mathcal{P}_{s,N}\binom{0}{1} = 0 \oplus \mathcal{P}_{s,N}$ and $\mathcal{P}_{s,N}\xi$ with $\mathbf{t}f\binom{0}{1} = \mathbf{t}\binom{0}{f} = f\xi$. Since $\mathbf{t}$ is invertible and preserves the symplectic form $\hat{\sigma}$, it follows that any maximally isotropic subspace is mapped onto a maximally isotropic subspace, which implies that $\mathcal{P}_{s,N}\xi$ is maximally isotropic. ■

As in the one dimensional case, we would like to have an easily checkable criterion for phase space vectors which guarantees that the above points are fulfilled, i.e. we need a corresponding property for reflection invariance. But, due to the existence of zero divisors, we are only able to give a necessary criterion:

Proposition 4.21 *Let $\xi = \mathbf{t}\binom{0}{1} \in \mathcal{P}_{s,N}^2$ be a column vector of a sympletic CA $\mathbf{t}$. Then $\overline{\xi} = \mu\xi$ with μ invertible and* $\gcd(\xi_+, \xi_-) = 1$.

Proof: We know there exists $\eta \in \mathcal{P}^2_{s,N}$ with $\hat{\sigma}(\eta,\eta) = 0$ and $\hat{\sigma}(\xi,\eta) = 1$. So if f is a common divisor of ξ_+ and ξ_- we write $\xi = f\tilde{\xi}$ and get $1 = \hat{\sigma}(\xi,\eta) = f\hat{\sigma}(\tilde{\xi},\eta)$, so f is invertible, which means we have $\gcd(\xi_+,\xi_-) = 1$.

Now lets have a look at

$$\begin{aligned} \xi_+ &= \xi_+\hat{\sigma}(\xi,\eta) = \xi_+(\overline{\xi}_+\eta_- - \overline{\xi}_-\eta_+) \\ &= \overline{\xi}_+(\xi_+\eta_- - \xi_-\eta_+) = \overline{\xi}_+\hat{\sigma}(\overline{\xi},\eta)\,. \end{aligned}$$

We used $\hat{\sigma}(\xi,\xi) = 0$ in the third equation. The same holds for ξ_- and we define $\overline{\mu} := \hat{\sigma}(\overline{\xi},\eta)$. Now we compute

$$\begin{aligned} \mu\overline{\mu} &= -\hat{\sigma}(\eta,\overline{\xi})\hat{\sigma}(\overline{\xi},\eta) \\ &= \eta_+\overline{\eta}_+\xi_-\overline{\xi}_- - \eta_-\overline{\eta}_+\xi_+\overline{\xi}_- + \eta_-\overline{\eta}_-\xi_+\overline{\xi}_+ - \eta_+\overline{\eta}_-\xi_-\overline{\xi}_+ \\ &= (\eta_+\overline{\xi}_- - \eta_-\overline{\xi}_+)\overline{\eta}_+\xi_- + \overline{\eta}_-\xi_+(\eta_-\overline{\xi_+} - \eta_+\overline{\xi}_-) \\ &= \hat{\sigma}(\overline{\eta},\overline{\xi})\overline{\eta}_+\xi_- + \overline{\eta}_-\xi_+\hat{\sigma}(\xi,\eta) = \overline{\hat{\sigma}(\xi,\eta)} = 1\,. \end{aligned}$$

We used the equation $\hat{\sigma}(\xi,\xi) = 0$ from the second to the third line and $\hat{\sigma}(\overline{\eta},\overline{\xi}) = \overline{\hat{\sigma}(\eta,\xi)} = -\hat{\sigma}(\xi,\eta) = -1$ in the last line and we have that μ is invertible. ■

Example 4.22 As an example of a translationally invariant stabilizer state, we consider translationally invariant graph states [Sch04]. The graph is encoded by its adjacency matrix $\Gamma = (\Gamma(x,y))_{x,x\in\mathbb{T}^s_N}$, and the isotropic subspace that determines the graph state is given by the phase space vectors

$$\begin{pmatrix} \Gamma f \\ f \end{pmatrix} \in \Xi_s = C_{\mathbb{F}}(\mathbb{T}^s_N)^2 \tag{4.50}$$

with $f \in C_{\mathbb{F}}(\mathbb{T}^s_N)$. Translation invariance of the graph state implies that the matrix elements $\Gamma(x,y)$ depend only on the difference $x-y$, so there is a function $\gamma \in C_{\mathbb{F}}(\mathbb{T}^s_N)$ such that $\Gamma(x,y) = \gamma(x-y)$ holds. Thus after Fourier transform the phase space vector, which generates the maximally isotropic subspace, is given by $\xi = \binom{\hat{\gamma}}{1}$ and we can choose a suitable symplectic cellular automaton $\mathbf{t}$ with $\xi = \mathbf{t}\binom{0}{1}$ by

$$\mathbf{t} = \begin{pmatrix} 1 & \hat{\gamma} \\ 0 & 1 \end{pmatrix}\,. \tag{4.51}$$

Figure 4.2 represents a translationally invariant graph state on the 1D torus $\mathbb{T}^1_6 = \mathbb{Z}_6$. The adjacency matrix Γ is given by

$$\Gamma = \begin{pmatrix} & & 1 & 1 & 1 & \\ & & & 1 & 1 & 1 \\ 1 & & & & 1 & 1 \\ 1 & 1 & & & & 1 \\ 1 & 1 & 1 & & & \\ & 1 & 1 & 1 & & \end{pmatrix} \tag{4.52}$$

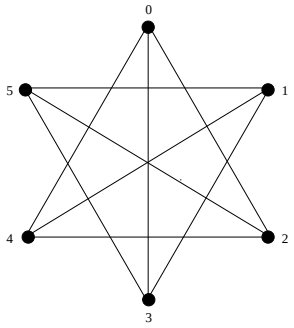

Figure 4.2: *A translationally invariant graph state on the 1D torus* $\mathbb{T}^1_6 = \mathbb{Z}_6$.

and obviously only depends on the difference $x - y$ of the variables $x, y \in \mathbb{Z}_6$. Applying the Fourier transform, yields the polynomial $\hat{\gamma} = u^2 + u^3 + u^4 = u^{-2} + u^2 + u^3$. The symplectic cellular automaton, which creates the graph state as explained above is given by the matrix

$$\mathbf{t} = \begin{pmatrix} 1 & u^{-2} + u^2 + u^3 \\ 0 & 1 \end{pmatrix} . \tag{4.53}$$

Note that $\mathbf{t}$ is reflection invariant, since $\overline{u^3} = u^3$ is a reflection fix-point. $\Diamond$

We are going to present another example to show that the phase space vectors do not have to be reflection invariant, because not all invertible elements are monomials. But the invertibility of a fixed polynomial depends on the size of the torus and so a fixed phase space vector ξ may define a translationally invariant stabilizer state for some N, but it is possible that there exists N', such that $\mathcal{P}_{1,N'}\xi$ is not maximally isotropic, and therefore ξ does not characterize a unique stabilizer state for N'.

Example 4.23 We consider for $p = 2$ the phase space vector

$$\xi = (1 + u + u^3)\begin{pmatrix} u^{-1} + u \\ 1 \end{pmatrix} \tag{4.54}$$

on a one dimensional torus of variable size. Note that $\hat{\sigma}(\xi, \xi) = 0$ holds for all N, so ξ generates an isotropic subspace. The corresponding tensor product of Pauli operators is given by

$$\mathbf{w}(\xi) = Z \otimes Y \otimes Y \otimes \quad \otimes X \otimes Z \, , \tag{4.55}$$

and is obviously not reflection invariant.

Let us first have a look at the case $N = 7$. It is easy to show that $1+u+u^3$ is not invertible. We define $\tilde{\xi} = \xi/(1+u+u^3) = \binom{u^{-1}+u}{1}$ and have that $\hat{\sigma}(\tilde{\xi}, \xi) = 0$, but $\tilde{\xi} \notin \mathcal{P}_{1,7}\xi$. So $\mathcal{P}_{1,7}\xi$ is not maximally isotropic, and there is no unique stabilizer state.

For $N = 6$ the inverse of $1+u+u^3$ is given by $u+u^4+u^5$, so ξ and $\tilde{\xi}$ generate the same subspace, which is actually maximally isotropic. So ξ is indeed a valid column of a symplectic automaton, but starting from the "all spins up" state both CQCAs corresponding to

$$\mathbf{t} = \begin{pmatrix} u+u^4+u^5 & (1+u+u^3)(u^{-1}+u) \\ 0 & (1+u+u^3) \end{pmatrix}, \quad \text{resp.} \quad \tilde{\mathbf{t}} = \begin{pmatrix} 1 & u^{-1}+u \\ 0 & 1 \end{pmatrix}$$

prepare the same stabilizer state. ◊

4.5 Conclusions

We have analyzed the structure of Clifford quantum cellular automata, where the results which can be achieved depend on the dimension of the lattice and whether we put periodic boundary conditions or working with the infinite lattice.

We have characterized the group of CQCAs in terms of symplectic cellular automata on a suitable phase space. With the help of Fourier transform, this phase space can be identified with two-dimensional vectors of Laurent-polynomials, and symplectic cellular automata can be described by two-by-two matrices with Laurent-polynomial entries. We have shown that these entries must be reflection invariant and that up to some global shift the determinant of the matrix must be one, so the group of CQCAs is isomorphic to the special linear group of two-by-two matrices with reflection invariant polynomials as matrix elements.

We have proven that there is a correspondence between 1D CQCAs and 1D translationally invariant stabilizer states. For a fixed translationally invariant pure stabilizer state $\omega^{\otimes\mathbb{Z}}$, which is in particular a product state, every other translationally invariant pure stabilizer state φ can be created by applying an appropriate CQCA T_φ to the chosen product state: $\varphi = \omega^{\otimes\mathbb{Z}} \circ T_\varphi$.

Pure stabilizer states can also be characterized by maximally isotropic subspaces. We have characterized the phase space vectors, which generate maximally isotropic subspaces, namely their components must be coprime and reflection invariant.

In the one-dimensional case we have also more clarified the group structure of CQCAs. As we have shown, each one-dimensional CQCA can be decomposed into a product of elementary shear automata and local Fourier transforms, so the group of CQCAs is generated by this set of operations.

For periodic boundary conditions the techniques from infinitely extended lattices can be applied to a certain extend. According to the discussion of translationally invariant stabilizer states on the 1D lattice, we have proven that there is an analogous correspondence between CQCAs and translationally invariant stabilizer states with periodic boundary conditions even in any lattice dimension.

Chapter 5

Invariance of Quantum Cellular Automata under All Lattice Symmetries

In this Chapter we study quantum cellular automata which, apart from translation invariance, also respect additional lattice symmetries, e.g. reflections and discrete rotations. We distinguish between direct invariance of the rules, which corresponds to a trivial representation of the symmetry group, and allowing additional one-site operations while transforming the lattice. In the first case we find that for many commonly used neighborhood schemes the class of covariant quantum cellular automata coincides exactly with the class of automata defined by a commuting unitaries scheme. In the case of non-trivial representations, we find that in one lattice dimension the index of a reflection covariant automaton must be trivial. In two lattice dimensions we find that the symmetry group is given by the dihedral group, and we study the symmetry restrictions on a quantum lattice gas, i.e., a automaton which is decomposed into a conditional shift and a single-site operation and which conserves the particle number.

5.1 Introduction

In many fields of physics it is common practice to assume some kind of symmetry, e.g. translation symmetry (also called *homogeneity*) or rotation symmetry (*isotropy*), and to study the restrictions on the system, which are imposed by the symmetry. Typically, this yields to a reduction of the parameter space and many calculations turn out to be only feasible by assuming symmetry. For instance, a prominent example in standard quantum mechanics is the calculation of eigenvalues of the hydrogen atom, where the Hamiltonian commutes with the angular momentum operators. In quantum information theory one of the main applications is the study of entanglement measures on symmetric states [VW01].

But also in classical mechanics or electrodynamics many problems are much easier solved when they are invariant under some symmetry. In classical mechanics symmetries can also be connected to conserved quantities by the Noether Theorem.

An important fact is that even under the restrictions of some symmetries complex physical behavior is possible. Indeed, this is one of the main purposes of both classical and quantum cellular automata. These may show complex behavior, although they can be described by rather simple local rules and the translation symmetry requires to use the same local rules throughout the lattice. But the underlying lattice of a cellular automaton dynamics usually provides more symmetries than translation symmetry, e.g. invariance under reflections and discrete rotations. Therefore, it is a natural question to ask, which restriction on the dynamics are imposed when we assume that these additional symmetries are also respected. Another motivation for doing this was the study of Clifford QCAs as presented in the foregoing Chapter. There, up to a global shift, the local rules turned out to be reflection invariant, although no such symmetry condition was postulated. This motivates to study general QCAs with such invariance conditions.

5.2 Covariance Conditions for QCAs

Apart from translation symmetry typical examples of lattice symmetries are invariance under reflections and discrete rotations. All these symmetries are described by linear functions on the lattice and the composition of two such functions is again a symmetry operation, i.e. we have a group structure. It is also interesting to study the combination of these symmetries together with the translation symmetry. Let therefore $\phi : \Gamma \to \Gamma$ be a linear function on some lattice Γ and $x \in \Gamma$ a translation vector. The action of the pair (ϕ, x) on some lattice point $y \in \Gamma$ is defined by $(\phi, x)y = \phi(y) + x$. Then it is easy to see that

$$(\phi, x) \circ (\phi', x') = (\phi\phi', \phi(x) + x') \tag{5.1}$$

holds. In particular, this means that we are concerned with a group of affine transformations (the *affine group*), where the multiplication of the elements is given by the semidirect product of Eq. (5.1). This motivates the following Definition.

Definition 5.1 *Symmetries of a lattice Γ are defined by a group G of linear functions $\phi : \Gamma \to \Gamma$. On the quasi-local algebra $\mathcal{A}(\Gamma)$ these symmetries are represented by automorphisms τ_ϕ such that (τ_ϕ, τ^x) is a representation of the affine group and*

$$\tau_\phi(\mathcal{A}_x) = \mathcal{A}_{\phi(x)} \tag{5.2}$$

holds. A quantum cellular automaton T on $\mathcal{A}(\Gamma)$ acts **covariantly with respect to the lattice symmetry** G*, if*

$$\tau_\phi \circ T = T \circ \tau_\phi \quad \forall \phi \in G\,. \tag{5.3}$$

One could think that Eq. (5.2) follows from (τ_ϕ, τ^x) being a representation of the affine group and is therefore unnecessarily postulated. But a simple example in one lattice dimension shows that this is not true: Suppose that σ is some translationally automorphism on $\mathcal{A}(\mathbb{Z})$ with $\sigma^2 = \mathrm{id}$ and define the reflection automorphism by $\tau_F(A_x) := \sigma(\tau^{-2x}A_x)$ for all $A_x \in \mathcal{A}_x$. A straightforward computation shows that $\tau_F \circ \tau^x = \tau^{-x} \circ \tau_F$ and $\tau_F^2 = \mathrm{id}$ hold, i.e., we have indeed a representation of the affine group, but it does not follow that $\tau_F(\mathcal{A}_0) \subset \mathcal{A}_0$ holds, because σ could be a QCA with non-trivial neighborhood scheme, e.g. a Clifford QCA.

Nevertheless, we find that the symmetry automorphisms are determined by its action on the centered cell.

Lemma 5.2 *The automorphisms τ_ϕ of a lattice symmetry $G \ni \phi$ are determined by $\tau_\phi|_{\mathcal{A}_0}$ and we have*

$$\tau_\phi(A_0) = U_\phi^* A_0 U_\phi \quad \forall A_0 \in \mathcal{A}_0\,, \tag{5.4}$$

where $U_\phi \in \mathcal{A}_0$ is a projective representation of G.

Proof: As usual, an automorphism is determined by its action on all single cell operators. Let therefore $A_x \in \mathcal{A}_x$, then we have

$$\tau_\phi(A_x) = \tau_\phi \circ \tau^x(\tau^{-x}A_x) = \tau^{\phi(x)}\tau_\phi(\underbrace{\tau^{-x}A_x}_{\in\mathcal{A}_0})\,.$$

$\tau_\phi|_{\mathcal{A}_0}$ is an automorphism on a finite dimensional matrix algebra and therefore unitarily implemented by some $U_\phi \in \mathcal{A}_0$. These unitaries must then form a projective representation of the symmetry group G, i.e., we have $U_\phi U_{\phi'} = \xi(\phi, \phi')U_{\phi\phi'}$ with some phase function ξ. ■

Clearly, a QCA T can only be covariant under some symmetry group G, if its neighborhood scheme is invariant under these symmetries. In detail, for the minimal neighborhood scheme $\mathcal{N}_x = \{y | [T(\mathcal{A}_x), \mathcal{A}_y] \neq 0\}$ we have $\mathcal{N}_x = \phi(\mathcal{N}_{\phi^{-1}(x)})$ for all $\phi \in G$. For the construction of covariant QCAs the single site support algebras

$$\mathcal{D}_x = S(T(\mathcal{A}_0), \mathcal{A}_x) \subset \mathcal{A}_x \tag{5.5}$$

will be very helpful. For those we have the following Lemma.

Lemma 5.3 *Let T be a QCA which is covariant with respect to a symmetry group G. Then the one-site support algebras fulfill*

$$\mathcal{D}_x = \tau_\phi(\mathcal{D}_{\phi^{-1}(x)}) \quad \forall \phi \in G\,. \tag{5.6}$$

Proof: Just a simple computation:

$$\begin{aligned} \mathcal{D}_x &= S(T(\mathcal{A}_0), \mathcal{A}_x) \\ &= S(T\tau_\phi(\mathcal{A}_0), \tau_\phi(\mathcal{A}_{\phi^{-1}(x)})) \\ &= \tau_\phi\, S(T(\mathcal{A}_0), \mathcal{A}_{\phi^{-1}(x)})\,. \end{aligned}$$

■

5.3 Trivial Representation of Lattice Symmetries

In this Section we study QCAs which are covariant with respect to the trivial representation with $U_\phi \equiv \mathbb{1}$ for all $\phi \in G$. The group G itself depends on the underlying lattice, but we assume that it contains all possible symmetry operations, e.g. the reflection in one lattice dimension, two reflections and rotations by $\pi/2$ for the lattice $\mathbb{Z}^2$, and analogously more reflections and rotations for the hexagonal lattice.

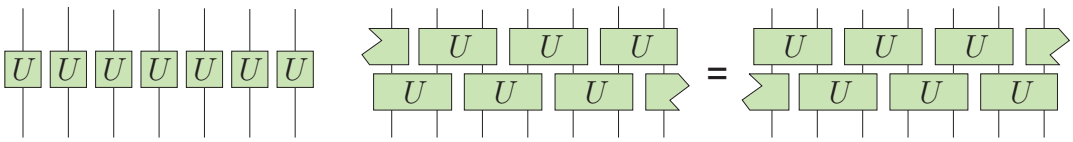

Figure 5.1: *Left: A QCA of single-site operations which is clearly reflection invariant. Right: The commuting unitaries can be organized in layers, where the order of the different layers doesn't matter.*

There are clearly some QCAs which are covariant under these assumptions, e.g. all translationally invariant single site operations, but also the class of QCAs defined by commuting unitaries (see Figure 5.1), possibly followed by a single site operation. The following Theorem states that for a certain kind of neighborhood schemes these are the only possibilities for covariant QCAs.

Theorem 5.4 *Suppose that T is a QCA with one of the following neighborhood schemes (see Figure 5.2):*

- *Nearest neighbor in one lattice dimension*

- *Von Neumann neighborhood in arbitrary dimensions*
- *Full neighborhood on a hexagonal lattice.*

Further, assume that T commutes with the automorphisms $\tau_\phi(A_x) = A_{\phi(x)}$ for all $\phi \in G$ and $A_x \in \mathcal{A}_x$. Then up to a one-site rotation T is a QCA which can be described by commuting unitaries (see Subsection 2.2.2).

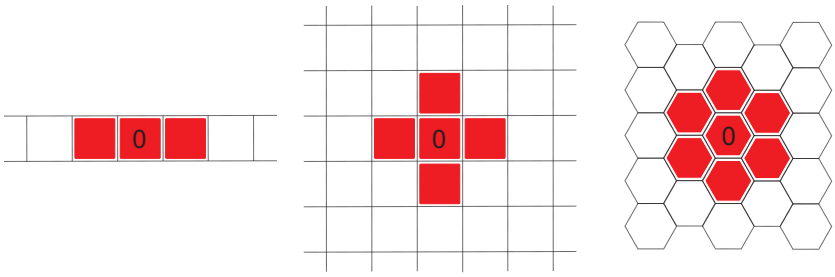

Figure 5.2: *Possible neighborhood schemes of Theorem 5.4.*

For the proof the following Lemma of [SW04] turns out to be very useful. For the proof see also [SW04].

Lemma 5.5 ([SW04]) *Suppose that all $\mathcal{D}_x$ for $0 \neq x \in \mathcal{N}$ are abelian. Then T is of the form $T(A_0) = W^* V_0^* A_0 V_0 W$ with $V_0 \in \mathcal{A}_0$ and the QCA defined by W alone is described by commuting unitaries.*

Proof of Theorem 5.4: With the help of the Lemma we only have to show that the support algebras $\mathcal{D}_x$ for $x \neq 0$ are abelian. First, note that by Lemma 5.3 we have $\mathcal{D}_x = \tau^{x-y}\mathcal{D}_y$ for all $x, y \in \mathcal{N} \setminus \{0\}$ because they can be transferred into each other by lattice symmetries. Now suppose we find lattice points $x_1 \neq x_2$ such that the neighborhood schemes $\mathcal{N} + x_1$ and $\mathcal{N} + x_2$ overlap in a single cell z. Since T is a homomorphism and by Lemma A.1, we then know that $\tau^{x_1}\mathcal{D}_{z-x_1}$ and $\tau^{x_2}\mathcal{D}_{z-x_2}$ have to commute. Because these algebras are shown to be equal, they have to be abelian. For the nearest neighbor case in one dimension and the von Neumann neighborhood scheme in arbitrary dimensions it is clear that there are two translates of the neighborhood scheme which overlap in a single cell, for the hexagonal case this is shown in Figure 5.3. ■

Note that all Clifford QCAs fulfill the requirements of the Theorem, provided they have one of the required neighborhood schemes[1]. This means that all such Clifford QCAs can be implemented by a scheme of commuting unitaries.

[1]In higher dimensions one should also assume that the rule is not essentially one-dimensional, i.e., the minimal neighborhood scheme should be of this kind.

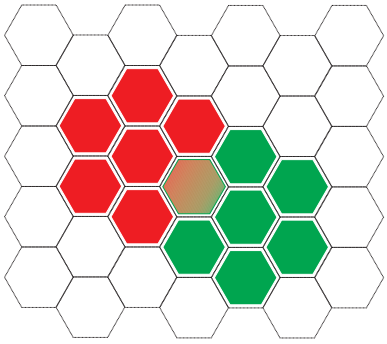

Figure 5.3: *The Figure shows that there are two translates of the neighborhood scheme, which overlap in a single cell as required for the proof of Theorem 5.4.*

For larger neighborhood schemes there are no corresponding results since the overlaps of the shifted neighborhood schemes get more complicated, e.g. for the Moore neighborhood there are no two translates which overlap in a single directly neighbored cell (this is only possible for the diagonal neighbors, but the lattice symmetries do not connect these cells with the directly neighbored ones, i.e., one only finds that the support algebras on the diagonal neighbored cells must be abelian). One can also see that Clifford QCAs with a Moore neighborhood may be much more complicated, e.g. they do not have to be invariant with respect to the $\pi/2$ rotations.

5.4 Non-trivial Representation of Lattice Symmetries

5.4.1 One Lattice Dimension

In one lattice dimension the only symmetry apart from translation symmetry is reflection invariance, i.e. invariance under the map $F : \mathbb{Z} \to \mathbb{Z}, x \mapsto -x$. On the quasi-local algebra we have therefore an automorphism τ_F with $\tau_F^2 = \mathrm{id}$ and a unitary U_F with $U_F^2 = \xi \mathbb{1}$ for some phase ξ. In Chapter 3 we have seen that a particular class of one-dimensional QCAs can be implemented in a Margolus partitioning scheme without local ancilla systems. This is exactly the subgroup of QCAs with trivial index, and here we show that all reflection invariant QCAs are contained in this subgroup and that the Margolus unitaries have to fulfill some covariance conditions.

Proposition 5.6 *Suppose T is a one-dimensional QCA which commutes with the reflection automorphism given by $\tau_F(A_x) = U_F^* A_{-x} U_F \in \mathcal{A}_{-x}$ for all $A_x \in \mathcal{A}_x$. Then we have* $\mathrm{ind}\, T = 1$ *and (in the nearest neighbor case) the unitaries of the*

Margolus partitioning scheme can be chosen such that they fulfill

$$[U, \mathbb{F}] = 0 \quad \textit{and} \quad \mathbb{F}V = V\mathbb{F}(U_F \otimes U_F)\,, \tag{5.7}$$

where $\mathbb{F}$ *denotes the Flip operator.*

Proof: Let $\mathcal{D}_+ = S(T(\mathcal{A}_0), \mathcal{A}_1)$, $\mathcal{D}_- = S(T(\mathcal{A}_1), \mathcal{A}_0)$, $\mathcal{E}_+ = S(T(\mathcal{A}_1), \mathcal{A}_1 \otimes \mathcal{A}_2)$ and $\mathcal{E}_- = S(T(\mathcal{A}_0), \mathcal{A}_{-1} \otimes \mathcal{A}_0)$. Then for the information flows (see Definition 3.2) we have

$$\begin{aligned} \mathcal{R} &= S(T(\mathcal{A}_0 \otimes \mathcal{A}_1), \mathcal{A}_1 \otimes \mathcal{A}_2) = (\mathcal{D}_+ \otimes \mathbb{1}) \vee \mathcal{E}_+ \\ \mathcal{L} &= S(T(\mathcal{A}_0 \otimes \mathcal{A}_1), \mathcal{A}_{-1} \otimes \mathcal{A}_0) = (\mathbb{1} \otimes \mathcal{D}_-) \vee \mathcal{E}_-\,. \end{aligned}$$

Similar to the case of the one-site support algebras (Lemma 5.3) one can compute that $\mathcal{D}_+ = \tau_F \tau^{-1} \mathcal{D}_-$ and $\mathcal{E}_+ = \tau_F \tau^{-1} \mathcal{E}_-$ hold. Therefore, we have $\mathcal{R} = \tau_F \tau^{-1} \mathcal{L} \cong \mathcal{L} \cong \mathcal{M}_d$ and $\operatorname{ind} T = 1$. From Theorem 3.6 it follows that the QCA can be implemented by a Margolus partitioning scheme without any local ancillary systems, i.e. by layers of unitaries U and V. The basis in the intermediate step can be chosen such that U commutes with the Flip operator. Let $\mathcal{D} = S(U^*(\mathcal{A}_0 \otimes \mathbb{1})U, \mathcal{A}_1) = S(U^*(\mathcal{A}_1 \otimes \mathbb{1})U, \mathcal{A}_0)$ and $\mathcal{E} = S(U^*(\mathcal{A}_0 \otimes \mathbb{1})U, \mathcal{A}_0) = S(U^*(\mathcal{A}_1 \otimes \mathbb{1})U, \mathcal{A}_1)$ (we think of these as subalgebras of the same matrix algebra, i.e. without distinguishing the localizations). Then we must have

$$\begin{aligned} V^*(\mathbb{1} \otimes \mathcal{D}) = \mathbb{1} \otimes \mathcal{D}_- \qquad &\text{and} \qquad V^*(\mathcal{D} \otimes \mathbb{1}) = \mathcal{D}_+ \otimes \mathbb{1}\,, \\ V^*(\mathbb{1} \otimes \mathcal{E}) = \mathcal{E}_- \qquad &\text{and} \qquad V^*(\mathcal{E} \otimes \mathbb{1}) = \mathcal{E}_+\,. \end{aligned}$$

Since with the relations from above we have $\mathcal{D}_- = U_F^* \mathcal{D}_+ U_F$ and $\mathcal{E}_- = (U_F \otimes U_F)^* \mathbb{F} \mathcal{E}_+ \mathbb{F} (U_F \otimes U_F)$, we get $V^* \mathbb{F}(\mathcal{E} \otimes \mathbb{1}) \mathbb{F} V = (U_F \otimes U_F)^* \mathbb{F} V^* (\mathcal{E} \otimes \mathbb{1}) V \mathbb{F} (U_F \otimes U_F)$ and similar equations for $\mathbb{1} \otimes \mathcal{E}, \mathcal{D} \otimes \mathbb{1}, \mathbb{1} \otimes \mathcal{D}$ which implies the required condition on V. ■

In many cases QCAs have a natural decomposition different from the Margolus scheme, e.g., a factorization into conditional shift operations and single-site operations. Since we are going to construct invariant QCAs in higher dimensions, which are decomposed in this way, we will also give such an example in one lattice dimension.

Example 5.7 We study a one-dimensional quantum lattice gas. The easiest way to describe the dynamics is a decomposition into two steps, but rather a decomposition into a single-site operation and a conditional shift step (see Subsection 2.2.2) than a Margolus partitioning scheme. The single cell structure is given by a tensor product, each describing some particle species, and the single-site operation describes the collision of different particle species. In the simplest

case[2] the single cell decomposes into two tensor factors $\mathcal{A}_0 = \mathcal{M}_2 \otimes \mathcal{M}_2$, where the two basis states in each factor label, whether the lattice site is occupied by the corresponding particle species or not. The conditional shift translates the first factor one position to the right and the other one to the left (see Figure 5.4).

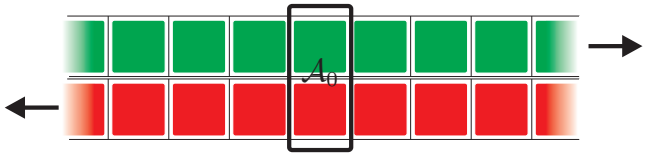

Figure 5.4: *Structure of a one-dimensional quantum lattice gas.*

This implies that the shift operation commutes with the reflection operation if U_F is equal to the flip on $\mathcal{A}_0$. The whole dynamics is then reflection invariant if the collision matrix also commutes with the flip. ◊

Similar to the case of the trivial representation one can also study the single-site support algebras. For instance, in the nearest neighbor case we have that $\mathcal{D}_{-1}$ and $\mathcal{D}_1 = U_F^* \mathcal{D}_{-1} U_F$ are isomorphic (and not equal as for the trivial representation). Nevertheless the algebras have to commute, which gives some constraints on the possible support algebras. The basic fact is that the algebras are, as finite dimensional C^*-algebras, isomorphic to a direct sum of full matrix algebras (see Proposition 2.1), i.e., we have $\mathcal{D}_1 \cong \bigoplus_n \mathcal{M}_{d(n)} \otimes \mathbb{1}_{d'(n)}$ with $\sum_n d(n)d'(n) = d$. A nearest neighbor QCA can only be reflection invariant if we find numbers $d(n), d'(n)$ such that the commutant $\mathcal{D}_1' \cong \bigoplus_n \mathbb{1}_{d(n)} \otimes \mathcal{M}_{d'(n)}$ contains an isomorphic copy of $\mathcal{D}_1$, i.e. we must have $U_F^* \mathcal{D}_1 U_F \subset \mathcal{D}_1'$.

We will study these restrictions in detail in the case $d = 3$. For two cell dimensions all nearest neighbor QCAs are classified in [SW04]. They are given by shifts, single-site operations and commuting unitaries, i.e., they are all reflection invariant unless they contain a shift component. For higher dimensions we cannot find similar results, e.g., the lattice gas example shows that for $d = 4$ there are QCAs which are not described by commuting unitaries (the support algebras $\mathcal{D}_1, \mathcal{D}_{-1}$ are both isomorphic to $\mathcal{M}_2 \otimes \mathbb{1}_2$ and therefore not abelian).

Proposition 5.8 *Suppose that T is a nearest neighbor QCA with single cell dimension $d = 3$, which commutes with a reflection automorphism. Then T can be described by a commuting unitaries scheme.*

Proof: For $d = 3$, apart from abelian ones, the only possible subalgebras are $\mathcal{M}_3$ itself and $\mathcal{M}_2 \oplus \mathbb{C}$. The commutant is then given by $\mathbb{C}\mathbb{1}_3$, respectively $\mathbb{C}\mathbb{1}_2 \oplus \mathbb{C}$. In particular both possible commutants are abelian and do therefore not contain

[2] See Chapter 6 for constructions of more complex lattice gas models.

an isomorphic copy of the algebra itself. This means a QCA with reflection symmetry is only possible when the support algebras $\mathcal{D}_{-1}, \mathcal{D}_1$ are abelian, which implies with Lemma 5.5 that we have a QCA of commuting unitaries. ■

5.4.2 Higher Lattice Dimensions

In this Subsection we focus on symmetries in higher lattice dimensions, mainly in two dimensions. The lattice should be build up of polygons of the same type, i.e. given by a regular tesselation of the plane. Note that this is only possible with triangles, squares and hexagons. Let us therefore consider two lattice dimensions and a QCA with von Neumann neighborhood, respectively a hexagonal lattice and full neighborhood scheme as in Figure 5.2. There are $k = 4$, respectively $k = 6$, reflections and rotations which leave the neighborhood scheme invariant (see Figure 5.5 for $k = 6$).

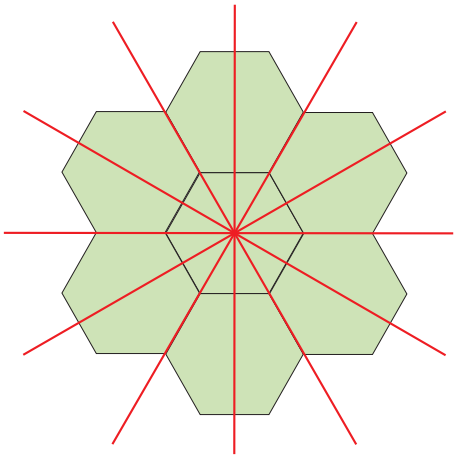

Figure 5.5: *Symmetry axis of a hexagonal lattice.*

The abstract symmetry group is given by the dihedral group[3] D_{2k}, i.e. the symmetry group of a regular polygon with k sides (see [Sim96] or any other textbook on finite groups). As already mentioned, the group consists of k reflections and k rotations and is clearly non-abelian because reflections and rotations do not commute in general. Nevertheless, the group is generated by just one reflection and one rotation. Let us verify this for the case $k = 4$. Consider the reflection $F : \mathbb{Z}^2 \to \mathbb{Z}^2, (x, y) \mapsto (x, -y)$ and the rotation $R : (x, y) \mapsto (-y, x)$. Then it is easy to see that the elements of D_8 are given by $\mathrm{id}, R, R^2, R^3, F, RF, R^2F, R^3F$, e.g., the reflection at the axis with $x = -y$ is given by R^3F.

Here we focus on the action of the group on the neighborhood cells. Clearly, a symmetry operation permutes the neighborhood cells except the centered one.

[3]Note that the notations D_k and Dih_k are also common.

Therefore, the dihedral group D_{2k} can be regarded as a subgroup of the symmetric group S_k, i.e., the group of all permutations of k elements. For the construction of covariant QCAs the irreducible representations of D_{2k} are interesting. The structure of those depends on whether k is even or odd. But since we are only interested in the cases $k = 4$ and $k = 6$, we only need the even case. Here we have four one dimensional irreducible representations and $k/2-1$ two dimensional representations [Sim96], which are given by

$$U_F = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad U_R = \begin{pmatrix} \cos 2\pi j/k & -\sin 2\pi j/k \\ \sin 2\pi j/k & \cos 2\pi j/k \end{pmatrix} \tag{5.8}$$

for $j = 1, \ldots, k/2-1$. For the construction of covariant QCAs we consider again a decomposition into conditional shifts and single-site operations. We show how particle number conservation and covariance under all lattice symmetries can reduce the parameters in the single-site collision matrix.

Example 5.9 We consider a quantum lattice gas on $\mathbb{Z}^2$ with von Neumann neighborhood scheme. The single cell is decomposed into a tensor product $\mathcal{A}_0 = \mathcal{M}_2^{\otimes 4}$ and the single cell support algebras are isomorphic to $\mathcal{M}_2$. In particular, we choose basis such that $\mathcal{D}_{(1,0)} = \mathcal{M}_2 \otimes \mathbb{1}^{\otimes 3}$, $\mathcal{D}_{(0,1)} = \mathbb{1} \otimes \mathcal{M}_2 \otimes \mathbb{1}^{\otimes 2}$, $\mathcal{D}_{(-1,0)} = \mathbb{1}^{\otimes 2} \otimes \mathcal{M}_2 \otimes \mathbb{1}$, $\mathcal{D}_{(0,-1)} = \mathbb{1}^{\otimes 3} \otimes \mathcal{M}_2$. The basis vectors of each algebra $\mathcal{M}_2$ are denoted by $|0\rangle$ and $|1\rangle$, describing whether the corresponding particle species occupies the lattice site or not. The dynamics is factorized into a conditional shift which translates the different particle species to their corresponding neighborhood sites, and a unitary collision matrix C describing the collision and reshuffling of the particle species. We suppose that this collision matrix conserves the particle number which means that it is decomposed into a direct sum of unitaries on the different particle number sectors.

The zero-particle sector is one-dimensional and should be invariant, the one-particle sector is spanned by the vectors $|1,0,0,0\rangle, |0,1,0,0\rangle, |0,0,1,0\rangle, |0,0,0,1\rangle$. The shift operation translates these vectors according to the structure of the single-site support algebras, e.g. the first one to the right. The action of the lattice symmetries on these vectors can then be described by a permutation, i.e., the representation of the reflection U_F exchanges the first and the third basis vectors and the rotation U_R is a cyclic permutation. In computational basis we therefore have

$$U_F = \begin{pmatrix} 0 & 0 & 1 & \\ 0 & 1 & 0 & \\ 1 & 0 & 0 & \\ & & & 1 \end{pmatrix} \quad \text{and} \quad U_R = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Now the one-particle component C_1 of the collision matrix is supposed to commute with both U_F and U_R. To study the resulting restriction on C_1, we transform

to a basis such that the representation decomposes into a direct sum of irreducible representations, e.g., we find a unitary V with

$$\tilde{U_F} = V^* U_F V = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix} \quad \text{and} \quad \tilde{U_R} = V^* U_R V = \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 0 & 1 \\ & & -1 & 0 \end{pmatrix}.$$

Now $\tilde{C_1} = V^* C_1 V$ should commute with $\tilde{U_F}$ and $\tilde{U_R}$, which implies that it is of the form $\tilde{C_1} = \mathrm{diag}(a, b, c, c)$ with $|a| = |b| = |c| = 1$. In computational basis the collision matrix then becomes

$$C_1 = \frac{1}{4} \begin{pmatrix} \tilde{a} & \tilde{b} & \tilde{c} & \tilde{b} \\ \tilde{b} & \tilde{a} & \tilde{b} & \tilde{c} \\ \tilde{c} & \tilde{b} & \tilde{a} & \tilde{b} \\ \tilde{b} & \tilde{c} & \tilde{b} & \tilde{a} \end{pmatrix} \tag{5.9}$$

with $\tilde{a} = a + b + 2c, \tilde{b} = a - b, \tilde{c} = a + b - 2c$, which is a well known result of [BT96]. In particular, the matrix is parameterized by three real parameters.

The two-particle sector C_2 can be handled similarly. Here we have the six basis vectors $|1,0,1,0\rangle, |0,1,0,1\rangle, |1,1,0,0\rangle, |0,1,1,0\rangle, |0,0,1,1\rangle, |1,0,0,1\rangle$ and the representation in this basis is given by

$$U_F = \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 0 & 1 & & \\ & & 1 & 0 & & \\ & & & & 0 & 1 \\ & & & & 1 & 0 \end{pmatrix} \quad \text{and} \quad U_R = \begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & 0 & 0 & 0 & 1 \\ & & 1 & 0 & 0 & 0 \\ & & 0 & 1 & 0 & 0 \\ & & 0 & 0 & 1 & 0 \end{pmatrix}.$$

A unitary transformation gives

$$\tilde{U_F} = \mathrm{diag}(1,1,1,-1,1,-1) \quad \text{and} \quad \tilde{U_R} = \mathrm{diag}(1,1,-1,-1) \oplus \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

which implies

$$\tilde{C_2} = \begin{pmatrix} a & \lambda\bar{b} \\ b & -\lambda\bar{a} \end{pmatrix} \oplus \mathrm{diag}(c, d, e, e)$$

with $|\lambda| = |c| = |d| = |e| = |a|^2 + |b|^2 = 1$, i.e. we have seven real parameters. In computational basis we then get

$$C_2 = \frac{1}{4} \left(\begin{array}{c|c} A & \sqrt{2}\lambda\bar{b} \\ \hline \sqrt{2}b & B \end{array} \right), \tag{5.10}$$

where A is a 2×2-matrix which is a linear combination of $\mathbb{1}$ and σ_z, B a 4×4-matrix with the same structure as C_1 and $\sqrt{2}\lambda\bar{b}$, respectively $\sqrt{2}b$, is a matrix where all elements are equal to $\sqrt{2}\lambda\bar{b}$, respectively $\sqrt{2}b$.

The three-particle sector works analogously to the case of the one-particle sector by exchanging the $|0\rangle$ and $|1\rangle$ state. The four-particle sector is one dimensional and is described by a collision phase. In total, all particle number conserving and lattice symmetry covariant collision matrices can be parameterized by 14 parameters within the set of all unitary 16×16-matrices, which is described by $16^2 - 1 = 255$ real parameters. In particular, only a small subset of all unitaries fulfill the desired symmetry conditions. $\Diamond$

5.5 Conclusions

We have studied various restrictions on quantum cellular automata, which are covariant with respect to lattice symmetries like reflections and discrete rotations. The action of the symmetry group on the quasi-local algebra is parameterized by a projective representation on the centered cell. If this representation is trivial, the only covariant QCAs with one of the neighborhood schemes of Figure 5.2 are exactly those defined by commuting unitaries. Choosing non-trivial representations allows the construction of more complex automata like quantum lattice gases. In one lattice dimension we have shown that all reflection covariant QCAs have trivial index, which allows the implementation in a Margolus partitioning scheme, where we also found some covariance conditions on the corresponding unitary layers. In two lattice dimensions the symmetry group of the lattice $\mathbb{Z}^2$, respectively the hexagonal lattice, is given by the symmetry group of a regular polygon with four, respectively six, sides, i.e. a dihedral group. We have used the irreducible representations of this group to compute the restrictions on the collision matrix of a covariant two-dimensional quantum lattice gas.

Part II

Quantum Walks

Chapter 6

Connecting Quantum Walks and Quantum Cellular Automata

In this Chapter we define quantum walks by the translationally invariant dynamics of a single particle on a lattice in discrete time, such that they can be identified with the one-particle sector of quantum cellular automata. Although we do not assume that a quantum walk is decomposed into coin toss and shift step, we show that such decompositions always exist in one lattice dimension. In principal, there are even different factorizations and these different decompositions are used for the construction of different quantum cellular automata, which reduce for a single particle to the same quantum walk. In particular, one of the constructions optimizes the single cell dimension of the resulting quantum cellular automaton, the other one the size of the neighborhood scheme. Finally, we compare the mean information flow, i.e. the indices, of the constructions.

6.1 Introduction

In this Chapter we want to study the connection between quantum walks and quantum cellular automata. We have analyzed the structure of QCAs in detail in the previous chapters, whereas we introduced quantum walks briefly in Chapter 2. To remember, a quantum walk describes the dynamics of one single quantum particle on a lattice in discrete time. In particular, both QWs and QCAs are dynamical systems in discrete time and space, which both act strictly local and usually also translationally invariant. But within the system of QCAs it is possible to describe the dynamics of many interacting particles, e.g., possibly there are even many particles per lattice site allowed.

But suppose that we start the evolution of a QCA with just one particle and that this QCA is particle number conserving, i.e., there will be exactly one particle throughout all time steps of the automaton. The dynamics of this single particle will then be translationally invariant and of finite propagation speed, i.e.

described by a quantum walk, possibly in a generalized form as defined in the following Section. A QW can therefore be identified with the *one-particle sector* of a (particle number conserving) QCA.

Vice versa, suppose we have some QW given and we want to construct a QCA out of the dynamics of the QW, i.e., the QW should describe the evolution of the QCA if we put just one particle on the lattice. Since a QCA acts local, the dynamics of several particles, which are far enough separated from each other, is also determined by the QW. But in the dynamics of a QCA it should be possible that particles meet. This means that we have to invent local interactions terms to make a quantum walk into a QCA rule, or to pass from a single particle to a, possibly interacting, diffusion. One solution, namely the non-interacting one, would be a second quantization of the QW, i.e., each cell is associated with a Fock space. But this would lead to infinite cell dimensions and corresponds to the structure of Gaussian quantum cellular automata as studied in [KW07]. Here we want to study QCAs with strictly finite cell dimension. Therefore, we cannot allow arbitrary particles to occupy the same cell, i.e. we have to invent some kind of "hard core interaction". Of course, there are many possibilities for doing this, leading to different cell dimensions and neighborhood schemes of the resulting QCA. We will present two basic construction methods, each optimizing one of these quantities.

For special cases the constructions are well known and have been introduced by Meyer [Mey96a]. Note that the structure, he calls quantum cellular automaton, corresponds to a quantum walk in the recent language, and he uses *quantum lattice gas automaton* for special QCA transformations with particle number conservation. Meyer also studied many properties of these transformations, both of the one-particle sector and of the lattice gas model [Mey97b, Mey97a, Mey98], and the possibility of simulating Schrödinger type evolutions with such a system was realized by Boghosian and Taylor [BT96, BT98]. But all these approaches rely on very special operations, and our results hold in much more general situations. For instance, our definition of quantum walks includes both the structure of Meyer's quantum cellular automata as well as the present definition of coined quantum walks.

The interesting matter of the close connection between QWs and QCAs is that QWs are an ideal test object for the implementation of QCAs. As mentioned in the introduction, QCAs are a powerful tool for implementing any quantum information task, especially for the simulation of many-body systems. In contrast, the power of QWs for doing such things is very limited, due to the possibility of solving the dynamics efficiently. Therefore, a long term goal in the recent experiments in optical lattices is the implementation of QCA like transformations with very high fidelity. To locate decoherence sources is one of the key points for realizing this goal. A possible way of doing this is to first let run a QW instead of a QCA, compare with the expected results, which are available due to the simulatability of QWs, and to suppress the upcoming decoherence effects. Indeed,

this way is pursued in the labs of Dieter Meschede and the theoretical study of decoherence in quantum walks in Chapter 8 is a further step for improvements.

6.2 Factorizations of Quantum Walks

In this Section we generalize the structure of quantum walks, in particular, we drop the correspondence between internal states and walking steps of the particle. So a quantum walk, which is generalized in this way, just describes the reversible and translationally invariant dynamics of a single particle in discrete time and space. In contrast, a constructive definition of quantum walks would allow all possible products of coin tosses and conditional shifts (compare to the definition of the Hadamard walk). Here we show that also in the general notion of QWs factorizations into these elementary operations exist, i.e., our axiomatic approach is in correspondence with the constructive definition of QWs.

As already mentioned in Section 2.3, it is because of translational invariance useful to describe quantum walks in momentum space. So in the one-dimensional case with d internal states we get unitary $d \times d$-matrices with elements, which are given by Laurent-polynomials with argument e^{ip}. In the standard case we have a constant unitary multiplied with a diagonal, momentum-dependent unitary, due to the correspondence between internal states and walking steps (compare with Section 2.3). Now this is exactly the point we want to generalize. We would like to describe a quantum walk on the s-dimensional cubic lattice $\mathbb{Z}^s$, which has d internal states per lattice site, just by a unitary $d \times d$-matrix consisting of Laurent-polynomials in the variables e^{ip_j} for $j = 1, \ldots, s$.

This situation is quite similar to the theory of lossless filter banks in electrical engineering and we can apply the same factorization techniques to quantum walks, which have been developed for so called paraunitary matrices. Note that a matrix $R(z)$ over Laurent polynomials in a general variable z is called paraunitary if the matrix is unitary for all z on the unit circle. We will use the factorization methods presented in [VD89, BJ99, XGS01].

Consider a unitary matrix $\hat{U}(p_1, \ldots, p_s)$ with Laurent-polynomial entries. A point $x \in \mathbb{Z}^s$ is called an element of the neighborhood of U, if the coefficient matrix of $e^{ix_1p_1} \ldots e^{ix_sp_s}$ does not vanish[1].

Lemma 6.1 *The determinant of a unitary matrix $\hat{U}(p_1, \ldots, p_s)$ with Laurent-polynomial entries is given by*

$$\det(\hat{U}) = \phi \prod_{j=0}^{s} e^{in_jp_j} \tag{6.1}$$

with some fixed phase ϕ.

[1]We use the denotation neighborhood accordingly to the neighborhood of a quantum cellular automaton.

Proof: Since $\hat{U}$ is unitary we have $1 = \det(\hat{U}\hat{U}^*) = \det(\hat{U})\overline{\det(\hat{U})}$, so the determinant of $\hat{U}$ is invertible. Of course the determinant is also a polynomial and with the invertibility we know that it must indeed be a monomial. ■

We refer to the tuple $(n_1, \ldots, n_s)$ of integers as the index of the walk for reasons which will become clear in Chapter 7. In the theory of filter banks this quantity is also called the McMillan degree of the matrix. From this Lemma it is clear that without internal degree of freedom the only possibilities for unitary quantum walks are (up to a global phase) shifts, which is a well known result of [Mey96b].

Now let us consider the one-dimensional case. We have

$$\hat{U}(p) = \sum_{x=L_-}^{L_+} U_x e^{ipx}\,, \tag{6.2}$$

where we assume that $U_{L_-}, U_{L_+} \neq 0$ and we call $L = L_+ - L_-$ the length of U. The index of $\hat{U}$ can range from dL_- to dL_+. The unitarity of $\hat{U}$ is equivalent to

$$\sum_x U_x^* U_{x+z} = \delta_{0,z} \mathbb{1}\,. \tag{6.3}$$

The partial shift on the first internal state is in momentum space given by

$$\tilde{S}(p) = \mathrm{diag}(e^{ip}, \underbrace{1, \ldots, 1}_{d-1})\,. \tag{6.4}$$

The following Proposition states that all quantum walks are generated by these simple conditional shifts and constant unitaries (coin tosses). The corresponding factorization theorem for filter banks is stated in [VD89, BJ99].

Proposition 6.2 *Let $\hat{U}(p)$ be a unitary $d \times d$ matrix over Laurent-polynomials in e^{ip} with index n. Then there exist unitary matrices $W_0, \ldots, W_{n+dL_-}$ such that*

$$\hat{U}(p) = e^{-ipL_-} W_0 \tilde{S}(p) W_1 \tilde{S}(p) \ldots W_{n+dL_--1} \tilde{S}(p) W_{n+dL_-}\,. \tag{6.5}$$

Proof: By extracting the global shift e^{-ipL_-} we can assume $L_- = 0$ and $L_+ = L$. Note that the index is thereby changed from n to $n + dL_-$. Eq. (6.3) then yields for $z = L$ the relation $U_0^* U_L = 0$ and, since $U_L \neq 0$, U_0 must be singular. Especially, there exists a vector $|\psi\rangle$ in the range of U_L, such that $PU_0 = 0$ for the one-dimensional projector $P = |\psi\rangle\langle\psi|$. We define $V(p) := \mathbb{1} - P(1 - e^{ip})$ and of course there exists a unitary W, such that $V(p) = W\tilde{S}(p)W^*$. Now have a look at the matrix

$$V(p)^* \hat{U}(p) = (\mathbb{1} - P)U_L e^{ipL} + \sum_{x=0}^{L-1} (U_x + P(U_{x+1} - U_x)) e^{ipx}\,. \tag{6.6}$$

The rank of the matrix $(\mathbb{1} - P)U_L$ is strictly less than the rank of U_L, because P is a projector onto a one-dimensional subspace of the range of U_L. Since the index of $V(p)$ is equal to one, the index of the righthand side of Eq. (6.6) is equal to $n + dL_- - 1$. By induction over the index the factorization follows. ■

This factorization method characterizes the generators of the group of local translationally invariant unitaries in one lattice dimension. Similar to the case of Clifford QCAs (see Theorem 4.16) the structure of the generators is quite simple.

There exists also an alternative factorization method, where the number of partial shifts is given by the length and not by the index [XGS01]. For this factorization we introduce the partial shift on r internal states by

$$S_r(p) = \mathrm{diag}(\underbrace{e^{ip}, \ldots, e^{ip}}_{r}, \underbrace{1, \ldots, 1}_{d-r}) \,. \tag{6.7}$$

Proposition 6.3 *Let $\hat{U}(p)$ be a unitary $d \times d$ matrix over Laurent-polynomials in e^{ip} with index n and length L. Then there exist constant unitaries $W_0, \ldots, W_{L+1}$ and integers r_j with $\sum_{j=0}^{L} r_j = n + dL_-$ such that*

$$\hat{U}(p) = e^{-ipL_-} W_0 S_{r_0}(p) W_1 S_{r_1}(p) \ldots W_L S_{r_L}(p) W_{L+1} \,. \tag{6.8}$$

Proof: Again we assume $L_- = 0$ and $L_+ = L$. We start with the relation $U_0^* U_L = 0$. This implies that we have for the images $\mathrm{im}(U_0) \cap \mathrm{im}(U_L) = \emptyset$ and we can decompose the coin Hilbert space $\mathcal{H}_C = \mathrm{im}(U_L) \oplus \mathrm{im}(U_0) \oplus \mathcal{H}_R$ with a remaining space $\mathcal{H}_R$. We define a unitary operation by

$$W(p)(\phi_L \oplus \phi_0 \oplus \phi_R) := e^{ip}\phi_L \oplus \phi_0 \oplus \phi_R \tag{6.9}$$

and we can find a constant unitary W_0 with $W(p) = W_0 S_{r_0} W_0^*$, where $r_0 = \mathrm{rank}(U_L)$.[2] So we get

$$W(p)^* \hat{U}(p) = U_0 + W(p)^* \sum_{x=1}^{L-1} U_x e^{ipx} + U_L e^{ip(L-1)}$$

and the length of this matrix is $L-1$. We apply this procedure iteratively until the length of the remaining matrix is zero and get a desired factorization. Obviously $\sum_{j=0}^{L} r_j$ is the index of the righthand side of Eq. (6.8) and so it must be equal to $n + dL_-$. ■

This factorization is quite similar to the factorization of Proposition 6.2, but the number of factors is in this case just given by the number of neighborhood

[2] We could also multiply ϕ_r with e^{ip}, which leads to $r_0 = d - \mathrm{rank}(U_0)$. This shows that the factorization is not unique.

sites of the quantum walk, whereas the number of "walking states" may differ in every factor.

In the case of qubits ($d = 2$) the factorization method of Proposition 6.3 coincides with a decomposition according to Proposition 6.2, because all S_r are equal to $\tilde{S}$. This means that in this case the bound on the number of factors is not optimal in Proposition 6.2.

Example 6.4 An often considered one-dimensional walk is the *Hadamard walk* with Hadamard coin $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and conditional shift $\mathrm{diag}(e^{ip}, e^{-ip})$. It can be decomposed into

$$\hat{U}(p) = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{ip} & 0 \\ 0 & e^{-ip} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = e^{-ip} \tilde{S}(p)^2 H \,. \tag{6.10}$$

$\Diamond$

It would be nice, if similar factorizations are also possible in higher lattice dimensions. In the theory of filter banks there are several attempts for doing this, but none of them corresponds exactly to our case. In [MLK77] it is shown that a matrix over Laurent polynomials in the two variables z_1, z_2 can be factorized according to the factors of its determinant, e.g. if the determinant of $R(z_1, z_2)$ decomposes into a product of Laurent polynomials $\prod_i f_i(z_1, z_2)$, then there exists a factorization $R(z_1, z_2) = \prod_i R_i(z_1, z_2)$ with $\det R_i = f_i$. In [KV90] it was conjectured that with this result a factorization similar to Proposition 6.2 is possible, but it is not clear that a paraunitary matrix R leads to paraunitary factors R_i, and in [DF04] this conjecture was indeed refuted. Up to now it seems that, similar to the case of Clifford QCAs (Subsection 4.3.3), the factorization results only hold in one lattice dimension.

6.3 Constructions of Quantum Cellular Automata

The idea for the construction of QCAs is to use the factorizations of the QW. These decompositions lead to simple elementary steps, which can be easily extended to a QCA step. Therefore, we construct QCA steps for each factor of the decomposition and multiply all these single QCA steps to the resulting QCA. Of course, one wants to build QCAs with smallest possible neighborhood scheme and smallest possible cell dimension. We find two constructions according to the two factorizations, each optimizing one of these quantities. First, we show how to construct QCAs with particle number conservation in general, afterwards we review the QCA construction for the well known example of the Hadamard walk [Mey96a].

6.3.1 Particle Number Conserving QCAs

Our construction methods are based on unilateral QCAs, i.e. the neighborhood is given by $\mathcal{N} = \{0, 1\}$ (or $\mathcal{N} = \{-1, 0\}$, respectively). The structure theorem in [SW04] (compare also to the implementation scheme from Chapter 3) states, that all such QCAs can be obtained by a simple concatenation of partial shifts and one-site rotations: First we apply a unitary one-site rotation U, which splits each cell into two subcells. In the second step one of the two subcells will be shifted to the right and a final one-site rotation V will be applied. The subcell structure will also be called intermediate step according to Fig. 6.1.

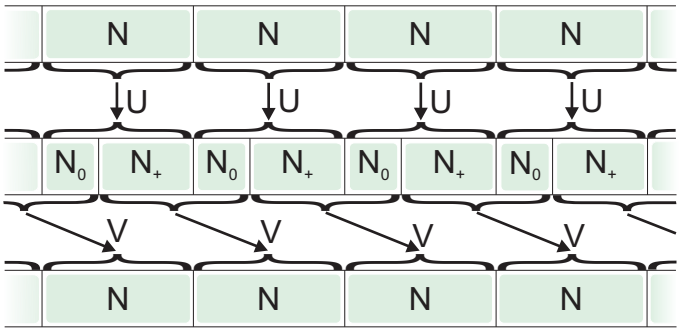

Figure 6.1: *Unilateral QCA with corresponding particle number operators. The partial shift and the unitary transformation V are summarized in a single step.*

Now we are looking for particle number conserving QCAs. Therefore, we introduce a local particle number observable $N^{(x)} = \tau^x(N)$ for each lattice-site x, when N is the particle number observable in cell 0. Of course, a unilateral QCA conserves the particle number, if the one-site rotations U and V are particle number conserving, i.e. U and V are decomposed into direct sums of unitaries with each of the summands acting on a fixed particle number. Therefore, we have to introduce particle number observables in the subcells, which we denominate by N_0 and N_+. Due to the unitarity of U and V the common spectrum of the particle number operators in the subcells must be equal to the spectrum of N in consideration of the multiplicities, i.e. we have

$$\mathrm{spec}(N) = \mathrm{spec}(N_0) + \mathrm{spec}(N_+)\,, \tag{6.11}$$

where the addition of the two families on the right hand side means addition in all possible combinations. With a little work it is also possible to show that all particle number conserving QCAs can be constructed by such a spectral decomposition [Vog05].

6.3.2 Hadamard Walk: A Prototype

We want to construct a nearest neighbor QCA, the one-particle sector of which simulates the Hadamard Walk. First we have to specify the single cell basis vectors of the QCA. Of course, we must take over the vectors $|R\rangle$ and $|L\rangle$. To describe cells, which are empty, we introduce a vacuum vector $|0\rangle$ in each cell, which will be invariant under the one-site unitaries, and we append a state $|RL\rangle$, which allows the collision of particles in one cell.

The best way to understand the construction, is to think of two bands (see also Figure 5.4), one containing the particles in state $|R\rangle$ and the other containing the particles in state $|L\rangle$. So each cell splits into two subcells corresponding to the walking direction of the particles. The conditional shift can easily be extended to this construction, just by shifting the two bands in the desired direction. The coin has to be extended to the state $|RL\rangle$, but there is only one phase left, because the coin should be unitary and respect the particle number. So in computational basis we get

$$\begin{pmatrix} 1 & & & \\ & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \\ & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & \\ & & & e^{i\phi} \end{pmatrix}. \tag{6.12}$$

In this case we have a one-site interaction of the walking particles, which is given by the collision phase ϕ. So if we put two particles on the lattice, one on an even and the other on an odd position, these particles are just doing the Hadamard Walk individually without any interaction. But in general one could also think of two-site interaction terms.

6.3.3 Optimizing Single Cell Dimension

We start with the factorization of Eq. (6.5), i.e.

$$\hat{U}(p) = e^{-ipL_-} W_1 \tilde{S}(p) W_2 \tilde{S}(p) \dots W_n \tilde{S}(p) W_{n+1}\,.$$

The factor e^{ipL_-} is just a global shift, which can be trivially extended to a QCA. The constant unitaries $W_1, \dots, W_{n+1}$ can be esteemed as coins, as the matrix $\tilde{S}(p)$ describes a conditional shift, translating one of the inner states to the right and leaving the other states on their sites, so we can distinguish one walking state from $d-1$ sitting states.

Now we take one of the factors $\tilde{S}(p)W_k$ and we want to build a QCA out of this QW. The neighborhood of this QW is given by $\{0,1\}$, and we want to have the same neighborhood for the QCA, i.e. a unilateral QCA. First we have to specify the internal states in each lattice-site. In this case we have d one-particle states and again we introduce a vacuum vector. It must be possible to split the spectrum of the particle number according to Eq. (6.11). Therefore,

we have to introduce two-particle states, but we don't have to allow all possible combinations. In particular, we allow two particles per site, merely if one of them is in the walking state and the other in any of the sitting states and not if both are in sitting states. So we end up with $d-1$ two-particle states and a single cell dimension of $2d$. We split the spectrum of N into $\mathrm{spec}(N_0) = (0, 1, \ldots, 1)$ (degeneracy of one-particle space is $d-1$) and $\mathrm{spec}(N_+) = (0, 1)$, so we can again think of two bands, one containing the walking particle species and the other one all sitting particle species. The construction of the QCA is again done in two steps. First we make a unitary one-site rotation, which respects the particle number. The one-particle block of this unitary is given by the coin W_k, as the two-particle block contains the interaction terms. The second step of the QCA is a conditional shift, translating the band with the walking particle species to the right and leaving the other invariant (see Fig. 6.2).

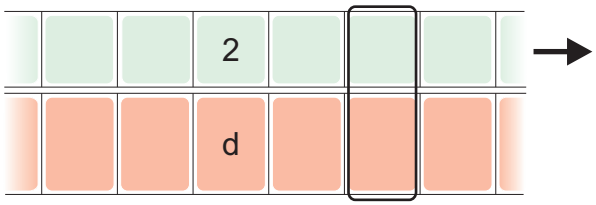

Figure 6.2: *QCA build from one of the factors. One QCA cell consists of two cells lying on top of each other.*

The whole QCA is up to a global shift and an additional one-site unitary given by the product of all these QCAs, so the total neighborhood is given by the sum of the neighborhoods of all the single factors. Since there are up to $d|\mathcal{N}_{QW}|$ of these factors, we get $\mathcal{N}_{QCA} \lesssim d\mathcal{N}_{QW}$. So this construction provides a small single cell dimension of $2d$, but in general the neighborhood blows up by a factor d.

Theorem 6.5 *For a QW with* $\dim \mathcal{H}_C = d$ *and neighborhood* $\mathcal{N}_{QW}$ *there exists a QCA with cell dimension* $2d$ *and neighborhood scheme* $\mathcal{N}_{QCA} \subseteq d\mathcal{N}_{QW}$*, which reduces to the dynamics of the QW when we run the QCA with a single particle.*

6.3.4 Optimizing Neighborhood Scheme

Here we start with the factorization of Eq. (6.8), i.e.

$$\hat{U}(p) = e^{-ipL_-} W_0 S_{r_0}(p) W_1 S_{r_1}(p) \ldots W_L S_{r_L}(p) W_{L+1} \,.$$

The drawback of this factorization is that we cannot mark a walking particle species, since the number of walking states may be different in each of the factors. So we have to allow that the number of walking particle species readjusts in each

factor. This is possible, if we take d bands, each containing one of the particle species. But this implies that we get up to d particles in each of the cells, e.g. if all bands are occupied at the same position. The spectrum of N can be decomposed into $(0,1) + \ldots + (0,1)$, where the sum is over all d bands, so we end up with a single cell dimension of 2^d. The spectrum of N_+, respectively N_0, gets r_k, respectively $d - r_k$, summands $(0,1)$, due to the structure of the conditional shift $S_{r_k}(p)$ (see Fig. 6.3).

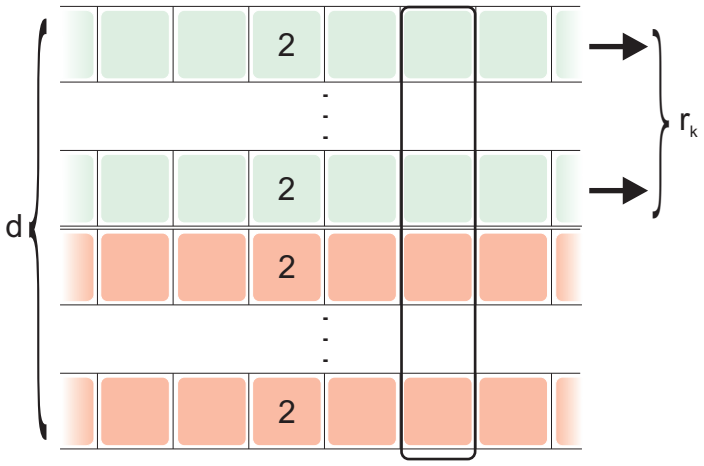

Figure 6.3: *QCA build from one of the factors. One QCA cell consists of d cells lying on top of each other.*

Analogously to the previous case, we construct a QCA for each factor $S_{r_k}(p)W_k$ in two steps. Again we first apply a unitary one-site rotation, leaving the particle number invariant. Of course the one-particle block is given by the coin W_k. But in this case we have to choose more unitaries for the higher particle numbers. The conditional shift is just given by a translation of the r_k bands, which contain the walking particle species.

This construction provides the smallest admissible neighborhood $\mathcal{N}_{QCA} = \mathcal{N}_{QW}$, but one has to pay with a larger single cell dimension of 2^d, i.e., on total we have the following result.

Theorem 6.6 *For a QW with* $\dim \mathcal{H}_C = d$ *and neighborhood* $\mathcal{N}_{QW}$ *there exists a QCA with cell dimension* 2^d *and neighborhood scheme* $\mathcal{N}_{QCA} = \mathcal{N}_{QW}$*, which reduces to the dynamics of the QW when we run the QCA with a single particle.*

Note that in the case of two internal states of the QW, e.g. the Hadamard walk, this construction is more efficient, since the single cell dimensions are equal in both construction methods. In general it is possible to combine both factorization and construction methods. But a decrease of the single cell dimension will lead to an increase of the neighborhood and vice versa, so we get a tradeoff

between these quantities. One can also think of other construction methods, but we assume that our constructions are optimal in a sense that it is in general not possible to get better bounds on the single cell dimension with a constraint of optimal neighborhood scheme or vice versa.

6.3.5 Comparison of Indices

In this Subsection we want to compare the information flows in the different constructions, i.e., we compute the indices of the different QCAs. Since these are decomposed into elementary shift steps, the computation of the indices is quite easy.

Proposition 6.7 *Let U be a quantum walk with index n, d-dimensional coin space and neighborhood scheme $\{L_-, \ldots, L_+\}$. Let T_{cell}, respectively T_{neigh}, be a QCA constructed from U according to Theorem 6.5, respectively Theorem 6.6. Then we have*

$$\operatorname{ind} T_{cell} = 2^n \left(\frac{2^{d-1}}{d}\right)^{L_-} , \tag{6.13}$$

$$\operatorname{ind} T_{neigh} = 2^n . \tag{6.14}$$

Proof: The single cell dimension of the QCA T_{cell} is $2d$ and this QCA is decomposed into a global shift by $-L_-$ positions (index: $(2d)^{-L_-}$) and $n + dL_-$ conditional shifts on the two-dimensional subsystem (index: 2). Note that the one-site unitaries do not contribute to the index. By the product formula ((ii) of Theorem 3.7) we have

$$\operatorname{ind} T_{cell} = (2d)^{-L_-} 2^{n+dL_-} .$$

The single cell dimension of T_{neigh} is given by 2^d and the QCA is decomposed into a global shift by $-L_-$ positions (index: 2^{-dL_-}) and L conditional shifts on subsystems of dimension 2^{r_k}. Since the sum of the r_k is according to Proposition 6.3 equal to $n + dL_-$, the result follows. ■

Remarkably, the index of the QCA T_{cell} does not only depend on the index of the walk. In particular, it is not even true in general that a trivial index of the walk (as you will see in the following Chapter, the index of a walk is trivial if it is equal to zero) implies a trivial index of the corresponding QCA. This is because the neighborhood is blown up only in one direction, e.g. in the presented construction only to the right. Of course, there is also an analogous construction blowing up the neighborhood to the left. In the formula for the index of T_{cell} one then has to replace L_- by L_+. Nevertheless, this construction seems to be more subtle, and the designation of essentially one walking particle species leads to very restricting interactions.

In contrast, the alternative construction T_{neigh} without blowing up the neighborhood scheme is more intuitive. Here the mean information flow in the QCA corresponds exactly to the mean information flow or mean group velocity of the QW (in the following Chapter we also find that the index of a walk is connected to the mean group velocity).

6.4 Conclusions

We have generalized the notion of quantum walks to the translationally invariant propagation of a single particle on a lattice. This generalization allowed us to identify quantum walks with one-particle sectors of particle number conserving QCAs. With this identification in mind, we discussed how to construct a QCA, when a QW, i.e., the dynamics of a single particle is given. Therefore, we introduced factorization methods, which decompose any QW into some elementary steps, namely coin tosses and conditional shifts. Note that these are exactly the operations which one would allow for a constructive definition of QWs, i.e., we have shown that our general approach fits to the constructive definition of QWs. In particular, the elementary QW operations can be straightforward extended to QCA operations. We have presented two factorization methods for QWs, which lead to two different constructions of QCAs. One of these constructions optimizes the single cell dimension by allowing only one walking particle species, which leads to an asymmetry in the information flow. The other construction method optimizes the neighborhood scheme of the resulting QCA, in particular, we get exactly the bound from the given QW.

Chapter 7

Index Theory of Quantum Walks

In this Chapter we introduce the index of a one-dimensional quantum walk by the trace of the difference of the half-axis projection and its image under the walk. We show that this quantity is an integer number and does not depend on the location of the half-axis, even when we do not assume translation symmetry for the walk. Further, we show that the index is additive under multiplication of quantum walks, i.e., the index is a homomorphism from the group of local unitaries into the additive group of integers. We also establish that only walks with trivial index can be locally deformed to the identity, i.e., one finds a continuous path within the set of local unitaries from the identity to the desired walk. In the translationally invariant case we find that the index is a measure for the mean group velocity of the system and corresponds to the winding number of the eigenvalues in momentum space. For translationally invariant walks we generalize most results also to higher lattice dimensions.

Some of the results of this Chapter are joint work with Annette Gattner.

7.1 Introduction

In Chapter 3 we have introduced the index theory for quantum cellular automata. In this Chapter we want to establish a corresponding index theory for quantum walks, e.g., we want to classify quantum walks up to local deformations. Again, we do not assume translation invariance for the general theory, i.e., we have different local evolutions on different lattice sites. As in the theory of quantum cellular automata we are interested in a locally computable quantity, which is constant along the line, even without assuming translation invariance, and which gives therefore rise to a global quantity.

A quantum walk is by definition a local unitary evolution, and therefore we do not have to look for local circuit schemes as in the QCA case. But some of the physical motivation for the QCA case can be transferred to the quantum walk case. For instance, it would be nice to know which local evolutions can be

combined to a global evolution, e.g. to answer if it is possible to combine a left shift on one part of the lattice and a right shift on another part. Furthermore, we would like to know which evolutions can be locally deformed into each other, i.e. without changing the global parameter. As in the QCA case we refer to this as *local equivalence*. In particular, the walks which are locally equivalent to the identity are of special interest, because these may be linked to continuous dynamics, i.e. to continuous time quantum walks introduced by Farhi and Gutmann [FG98] (see also [Kem03]) rather than many-particle systems compared to the QCA case.

As mentioned in Section 2.3, the asymptotic behavior is determined by the velocity distribution of the initial state [GJS04b]. Here we do not look at the velocity of a single particle, but rather for a "global drift" of the system: we connect the index with the *mean velocity* of the system, i.e. the velocity of the particle averaged over all input states localized at a single cell. This can be interpreted as the analogue of the mean information flow of a quantum cellular automaton.

The mathematical motivation is the same as in the QCA case, i.e., we want to find the connected components within the group of quantum walks. But the mathematical tools are very different in this case. For instance, it turns out that the difference of a half-axis projector and its image under the walk is a very important operator. Such a difference of projections in an infinite dimensional space have been considered by Avron, Seiler and Simon in [ASS94b] and the same authors used this theory for a rigorous study of the quantum Hall effect [ASS90, ASS94a]. Note that they also use the denotation *index*, whereas Kitaev uses the denotation *flow* for a corresponding quantity in [Kit05].

7.1.1 Outline and Summary of Results

In the following Section we first define the index of a local unitary in an elementary way, just by regarding some of the matrix elements. We show that the index formula can be rewritten by considering the projection onto the positive half axis and its image under the local unitary, which allows us to use the powerful index theory of pairs of projections [ASS94b]. We review this theory in Section 7.3, where we also demonstrate the connection to the index theory of Fredholm operators.

In Section 7.4 we apply the index theory of projections to the index of quantum walks, i.e. to the quantity defined in Section 7.2. We find that the results are similar to the case of quantum cellular automata (compare Chapter 3). For instance, the index quantity is additive (for QCAs: multiplicative) under multiplication and composition of quantum walks, and only the walks with trivial index can be decoupled by a local unitary and contracted to the identity.

For quantum walks with translation symmetry we study some relations in more detail in Section 7.5, e.g. we find that the index can be connected with the

determinant of the Fourier transform of the walk, as we already indicated in the previous Chapter. We also find that the index corresponds to the mean group velocity of the walk and to the winding number of the eigenvalues. Note that in the translationally invariant case the results can mainly be generalized to higher lattice dimensions (see Subsection 7.5.1).

7.2 Basic Definitions

Since we do not assume translation invariance for the general theory of this Chapter, we first describe how the notion of quantum walks differs from Section 2.3 and from the previous Chapter in this case. We have a spatial degree of freedom labeled by lattice points $x \in \mathbb{Z}$ and to each lattice point we associate a finite dimensional Hilbert space $\mathcal{H}_x$. The total Hilbert space is then given by the direct sum of these, i.e.

$$\mathcal{H} = \bigoplus_{x=-\infty}^{\infty} \mathcal{H}_x \,. \tag{7.1}$$

For a unitary operator U on such a direct sum we have a block matrix decomposition $U_{xy} : \mathcal{H}_y \to \mathcal{H}_x$ given by

$$U \bigoplus_y \phi_y = \bigoplus_x \sum_y U_{xy}\phi_y \,. \tag{7.2}$$

Furthermore, a quantum walk is assumed to be *local*, which means that for any y only finitely many U_{xy} are nonzero, i.e. there is some $L < \infty$ such that $U_{xy} = 0$ for all $x < y - L$ and $x > y + L$.

The usual translationally invariant case arises when all $\mathcal{H}_x \equiv \mathcal{H}_0$ are of the same dimension. The total Hilbert space then becomes $\mathcal{H} \cong \ell^2(\mathbb{Z}) \otimes \mathcal{H}_0$, and the walk commutes with the shift operations

$$S^x(|y\rangle \otimes \phi_0) = |x + y\rangle \otimes \phi_0 \,. \tag{7.3}$$

Without translation invariance it is quite natural to drop the distinction between internal degrees of freedom and spatial degree of freedom in each $\mathcal{H}_x$ (with basis vectors $|x, 1\rangle, \ldots, |x, d_x\rangle$). For instance, we can "flatten" the internal structure by labeling the basis vectors of $\mathcal{H}$ by a single integer parameter in the sequence

$$\ldots, |x-1, d_{x-1}\rangle, |x, 1\rangle, \ldots, |x, d_x\rangle, |x+1, 1\rangle, \ldots \,,$$

i.e., we can assume without loss of generality that $\mathcal{H}_x = \mathbb{C}$ and $\mathcal{H} = \ell^2(\mathbb{Z})$ holds. Of course, by flattening the structure the neighborhood increases, and vice versa grouping of basis vectors to subspaces $\mathcal{H}_x$ can be done, e.g., to get strictly nearest neighbor dynamics, or to have strict translation invariance rather than invariance with respect to some power of the shift.

On the Hilbert space $\ell^2(\mathbb{Z})$ a quantum walk can be seen as an infinite dimensional unitary matrix where, according to locality, only the entries close to the diagonal are nonzero, i.e., the matrix is of the form

$$U = \left(\begin{array}{cc|cc} \ddots & & u_{0,-L} & \\ & \ddots & u_{1,-L+1} \ddots & 0 \\ & u_{-1,-1} & u_{0,-1} \quad u_{L-1,-1} & \\ \hline u_{-L,0} \cdots u_{-1,0} & & u_{0,0} \cdots \cdots u_{L,0} & \\ u_{-L+1,1} \ddots & & u_{1,1} \ddots & \\ \ddots u_{-1,L-1} & & & \\ 0 & & u_{0,L} \ddots & \\ & & & \end{array}\right), \tag{7.4}$$

where the through lines are drawn according to the following definition of the index: We only consider the entries in the off-diagonal blocks to define the index by

$$\operatorname{ind} U := \sum_{y<0\leq x} |u_{xy}|^2 - |u_{yx}|^2 \,, \tag{7.5}$$

and due to locality this is a strictly finite sum. This definition is due to Kitaev [Kit05], who calls this the *flow* of a local unitary. Note that the off-diagonal blocks are exactly those which connect the left and right axis, i.e., the index quantizes, similar to the case of quantum cellular automata, the difference of information going from left to right and from right to left, respectively.

This formula can easily be generalized if we do not assume that the Hilbert spaces $\mathcal{H}_x$ are trivial. In the block matrix decomposition (7.2) we find

$$\operatorname{ind} U = \sum_{y<0\leq x} \operatorname{tr}(U_{xy}^* U_{xy}) - \operatorname{tr}(U_{yx}^* U_{yx}) \,. \tag{7.6}$$

Nevertheless, this quantity does not depend on the grouping into subspaces $\mathcal{H}_x$ since the operator product and the trace imply the correct sum over the internal basis labels of $\mathcal{H}_x$ and $\mathcal{H}_y$. Clearly, in the case of $\mathcal{H}_x = \mathbb{C}$ Eq. (7.6) reduces to (7.5).

Although the Formulas (7.5) and (7.6) describe the easiest way to compute the index for any given local unitary, they are not so suitable for getting the key

properties. Therefore, we consider the projector P onto the positive half axis, i.e. the projection onto the subspace $\bigoplus_{x\geq 0}\mathcal{H}_x$. Then, for $\phi_{x,y}\in\mathcal{H}_{x,y}$ we have

$$\langle\phi_x|UP-PU|\phi_y\rangle=\begin{cases}0 & ,x\geq 0 \text{ and } y\geq 0\\ \langle\phi_x|U_{xy}|\phi_y\rangle & ,x<0 \text{ and } y\geq 0\\ -\langle\phi_x|U_{xy}|\phi_y\rangle & ,x\geq 0 \text{ and } y<0\\ 0 & ,x<0 \text{ and } y<0\end{cases}, \tag{7.7}$$

i.e., we get exactly the signs used in the definition of the index.

Definition 7.1 *Let U be a local unitary on a Hilbert space of the form (7.1) and P the projection onto the subspace $\bigoplus_{x\geq 0}\mathcal{H}_x$. Then the* **index of a quantum walk** *U is defined by*

$$\operatorname{ind} U:=\operatorname{tr}(U^*[U,P])=\operatorname{tr}(P-U^*PU)\,, \tag{7.8}$$

which is due to Eq. (7.7) equivalent to Formula (7.6).

Note that we cannot use the linearity of the trace in Eq. (7.8) to write the right hand side as a difference of two terms, because the trace of the projections itself does not exist, i.e. we would get an indeterminate expression $\infty-\infty$.

This definition connects the index with the difference of the two projections P and U^*PU. In particular, we can use the powerful theory of [ASS94b] to make statements about fundamental properties of the index for quantum walks.

7.3 Index Theory of Pairs of Projections

In this Section we give an overview on the results of [ASS94b], because we will apply these directly to the index of quantum walks as defined in the previous section. The theory even works in a more general situation, e.g. we just assume that we have two projections P and Q without requiring that these are linked by a quantum walk. The only assumption is that the difference $P-Q$ is compact (in Subsection 7.3.2 this condition will even be more relaxed). Note that in our case $Q=U^*PU$ holds and that the difference $P-Q$ is, due to locality of U, of finite rank and therefore in the trace class. Although some of the results can be proven more directly in our situation, we will present the general theory which may allow to generalize our results for quantum walks to more general situations such as approximately local dynamics. We will leave the study of these possibilities for future work.

Before going to the index theory, we will state some of the algebraic properties of two projections P and Q, which directly follow from the relation $P^2=P$ for projections. First, note that the square of the difference operator $P-Q$ commutes with both P and Q, i.e.

$$[(P-Q)^2,P]=[(P-Q)^2,Q]=0\,. \tag{7.9}$$

Kato [Kat66] introduced a second operator $\mathbb{1} - P - Q$. Since $\mathbb{1} - P$ is also a projection, the square of this operator also commutes with P and Q. Furthermore, we have that both squares add up to the identity

$$(P - Q)^2 + (\mathbb{1} - P - Q)^2 = \mathbb{1}\,, \tag{7.10}$$

where the operators themselves anti-commute, i.e.

$$(P - Q)(\mathbb{1} - P - Q) + (\mathbb{1} - P - Q)(P - Q) = 0\,. \tag{7.11}$$

7.3.1 General Theory

As already mentioned, we are interested in the difference $P - Q$ of a pair of projections (P, Q). Assume that the difference is a compact operator, i.e., one which can be approximated by operators of finite rank (for the general theory of compact operators we refer to [Wei80], or any other textbook on linear operators in Hilbert space). In an infinite dimensional space the spectrum of such an operator consists, apart from zero, of at most countably many eigenvalues, possibly accumulating at zero. This means that for all $\lambda \neq 0$ the eigenspaces, i.e. the spaces $\ker(P - Q - \lambda\mathbb{1})$, are finite dimensional. For the definition of the index of the pair (P, Q) we only need the dimensions of the eigenspaces to eigenvalues ± 1.

Definition 7.2 *Let P and Q be a pair of projections on a Hilbert space $\mathcal{H}$. Suppose that the difference $P - Q$ is compact. Then the* **index of the pair of projections** *(P, Q) is defined by*

$$\mathrm{ind}(P, Q) := \dim\ker(P - Q - \mathbb{1}) - \dim\ker(P - Q + \mathbb{1})\,. \tag{7.12}$$

Clearly, the index is an integer number and $\mathrm{ind}(P, Q) = -\mathrm{ind}(Q, P)$ holds. It is also obvious that the index is invariant under unitary transformations, i.e.

$$\mathrm{ind}(U^*PU, U^*QU) = \mathrm{ind}(P, Q) \tag{7.13}$$

for any unitary $U \in \mathcal{B}(\mathcal{H})$. Note that the projections P and Q are positive with $\|P\|, \|Q\| \leq 1$. Therefore the kernels can be rewritten by

$$\ker(P - Q - \mathbb{1}) = \mathrm{ran}\, P \cap \ker Q \quad \text{and} \quad \ker(P - Q + \mathbb{1}) = \mathrm{ran}\, Q \cap \ker P\,. \tag{7.14}$$

These relations help us to show that the index is additive, i.e. for a sum of two operators the index is equal to the sum of the individual indices:

Proposition 7.3 ([ASS94b]) *Let P, Q, R be projections and both $P - Q$ and $Q - R$ compact. Then we have*

$$\mathrm{ind}(P, R) = \mathrm{ind}(P, Q) + \mathrm{ind}(Q, R)\,. \tag{7.15}$$

Proof: Clearly, the sum of two compact operators is compact, i.e. the index for (P, R) exists. The sum formula can then be shown by Relation (7.14) and decomposing the projection P into $P|_{\ker Q \cap \ker R} \oplus P|_{\ker Q \cap \mathrm{ran}\, R} \oplus P|_{\mathrm{ran}\, Q \cap \ker R} \oplus P|_{\mathrm{ran}\, Q \cap \mathrm{ran}\, R}$. ■

In the following Theorem we find an interchanging unitary operator, if the index of (P, Q) is trivial. Such a unitary will play an important role for the theory of quantum walks.

Theorem 7.4 ([ASS94b]) *Let (P, Q) be a pair of projections with $P - Q$ compact. Then there exists a unitary operator V, which interchanges P and Q, i.e.,*

$$V^*PV = Q \quad \textit{and} \quad V^*QV = P \tag{7.16}$$

if and only if $\mathrm{ind}(P, Q) = 0$.

Proof: First, suppose that such a unitary exists. Then we have $V^*(P - Q)V = Q - P$ and for the index $\mathrm{ind}(P, Q) = \mathrm{ind}(Q, P) = -\mathrm{ind}(P, Q)$, which then has to be zero.

Now, suppose $\mathrm{ind}(P, Q) = 0$ holds and let $R_\pm$ be the projectors onto the spaces $\ker(P - Q \mp \mathbb{1})$ and $R_0 = \mathbb{1} - R_+ - R_-$. Since the index vanishes, the spaces $\mathrm{ran}(R_+)$ and $\mathrm{ran}(R_-)$ have the same dimension and we can find a unitary $U_0 : \mathrm{ran}(R_+) \to \mathrm{ran}(R_-)$. Define $V_0 : \mathrm{ran}(R_+) \oplus \mathrm{ran}(R_-) \to \mathrm{ran}(R_+) \oplus \mathrm{ran}(R_-)$ by $V_0(\varphi \oplus \psi) = U_0^*\psi \oplus U_0\varphi$, i.e. a vector from $\mathrm{ran}(R_+)$ is mapped to $\mathrm{ran}(R_-)$ and vice versa.

In the following paragraph we let all operators be restricted to $\mathrm{ran}(R_0)$. Let $B = \mathbb{1} - P - Q$ and $A = P - Q$. Then we can define in accordance to Eq. (7.10) the operator $|B| = \sqrt{\mathbb{1} - A^2}$, which is strictly positive, because $\|A\| < 1$ holds with the restriction onto $\mathrm{ran}(R_0)$. Let $V_1 : \mathrm{ran}(R_0) \to \mathrm{ran}(R_0)$ be the unitary with $V_1 = \mathrm{sign}(B) = |B|^{-1}B$. Clearly, V_1 commutes with B, i.e., we have $V_1^*(P + Q)V_1 = P + Q$. Now A and B anti-commute by Eq. (7.11) and, since $|B|$ and A commute, V_1 and A anti-commute, i.e., we have $V_1^*(P - Q)V_1 = Q - P$ and, with the relation from above, V_1 interchanges P and Q on the subspace $\mathrm{ran}(R_0)$.

The operator $V = V_0 \oplus V_1$ on $\mathrm{ran}(R_+) \oplus \mathrm{ran}(R_-) \oplus \mathrm{ran}(R_0) = \mathcal{H}$ then fulfills $V^*PV = Q$ and $V^*QV = P$ as required. ■

7.3.2 Connection to the Fredholm Index

In this Subsection we will show the connections to the index theory of Fredholm operators, which is applicable in an even more general situation. The readers, who are not interested in this, can just skip this without missing important facts for the following sections. For the theory of Fredholm operators see the appendix of [ASS94b] and also the book of Kato [Kat66].

A Fredholm operator C from one Hilbert space $\mathcal{H}_1$ to another one $\mathcal{H}_2$ is possibly unbounded but closed, i.e., the graph of F is closed.

Definition 7.5 *A closed operator $C : \mathcal{H}_1 \to \mathcal{H}_2$ is called a* **Fredholm operator** *if the following conditions are fulfilled*

(*i*) $\mathrm{ran}(C)$ *is closed.*

(*ii*) $\ker(C)$ *is finite dimensional.*

(*iii*) $\mathrm{ran}(C)^\perp$ *is finite dimensional.*

One then defines the **Fredholm index** *by* $\mathrm{ind}_F(C) = \dim\ker(C) - \dim\mathrm{ran}(C)^\perp$.

With the results of Deift [Dei78] it follows that a closed operator C is a Fredholm operator if and only if zero is neither in the essential spectrum of C^*C nor of CC^*. The following Theorem connects the index of projections (P, Q) with the Fredholm index of the product QP.

Theorem 7.6 ([ASS94b]) *Let P, Q projections and $C = QP$ viewed as a map from* $\mathrm{ran}(P)$ *to* $\mathrm{ran}(Q)$*. Then C is Fredholm if and only if*

(*i*) 1 *and* -1 *are isolated points of* $\mathrm{spec}(P - Q)$*;*

(*ii*) $\ker(P - Q \mp \mathbb{1})$ *are both finite dimensional.*

Furthermore, we have

$$\mathrm{ind}_F(C) = \dim\ker(P - Q - \mathbb{1}) - \dim\ker(P - Q + \mathbb{1}) = \mathrm{ind}(P, Q)\,. \qquad (7.17)$$

Sketch of proof: We will give only a rough sketch of the proof (see [ASS94b] for a full version). First, note that

$$\begin{aligned} \ker(C) &= \mathrm{ran}(P) \cap \ker(Q) = \ker(P - Q - \mathbb{1})\,, \\ \mathrm{ran}(C)^\perp &= \mathrm{ran}(Q) \cap \ker(P) = \ker(P - Q + \mathbb{1}) \end{aligned}$$

holds, i.e. the index formula (7.17) is true once the equivalence is shown.

Suppose that C is a Fredholm operator and ψ_n an orthonormal sequence with $\|(P - Q - \mathbb{1})\psi_n\| \to 0$. Then $\|P\psi_n\| \to 1$ and $\|Q\psi_n\| \to 0$ must hold. So $\varphi_n =$

$P\psi_n/\|P\psi_n\|$ is a sequence with $(C^*C)\varphi_n = (PQP)\varphi_n \to 0$, so $0 \in \sigma_{ess}(C^*C)$. Since C is a Fredholm operator such a sequence cannot exist, i.e. $1 \notin \sigma_{ess}(P-Q)$. Similarly, $-1 \notin \sigma_{ess}(P-Q)$, which is then equivalent to $(i)+(ii)$.

Let (i) and (ii) hold. Then we can write $P-Q = F_1 + F_2$, where F_2 is finite rank and $F_2 \leq (1-\epsilon)\mathbb{1}$ for some $\epsilon > 0$. We get $PQP = -PF_2P + P(1-F_1)P \geq -PF_2P + \epsilon P$ and therefore $0 \notin \sigma_{ess}(C^*C)$. □

7.3.3 Trace Formula

In the situation of quantum walks, i.e. strictly local unitaries, the difference $P-Q$ is a finite rank operator and, in particular, a trace class operator and we defined the index by the trace of $P-Q$. The following Theorem tells us that this quantity is equal to the index of (P,Q). We only have to show that all non-zero eigenvalues apart from ± 1 occur in pairs $\pm\lambda$ with equal dimension of eigenspaces for $+$ and $-$. So these eigenvalues will not contribute to the trace.

Theorem 7.7 ([ASS94b]) *Suppose that $P-Q$ is a trace class operator. Then we have*

$$\mathrm{ind}(P,Q) = \mathrm{tr}(P-Q)\,. \tag{7.18}$$

Proof: Fix $0 < \lambda < 1$ and let $\mathcal{H}_{\pm\lambda} = \{\psi | (P-Q)\psi = \pm\lambda\psi\}$. As already mentioned we will show that $\dim \mathcal{H}_{+\lambda} = \dim \mathcal{H}_{-\lambda}$ holds. Since $B = \mathbb{1} - P - Q$ anti-commutes with $P-Q$ (Eq. (7.11)), B maps $\mathcal{H}_{+\lambda}$ to $\mathcal{H}_{-\lambda}$. Restricted to $\mathcal{H}_{+\lambda}$ we have $B^2 = \mathbb{1} - (P-Q)^2 = (1-\lambda^2)\mathbb{1}$ according to Eq. (7.10). Thus B is an invertible map of $\mathcal{H}_{+\lambda}$ to $\mathcal{H}_{-\lambda}$, i.e. the dimensions are equal. ■

The same argument holds when the operator $(P-Q)^{2n+1}$ is only trace class for sufficiently large n. In this case we get

$$\mathrm{ind}(P,Q) = \mathrm{tr}((P-Q)^{2n+1})\,. \tag{7.19}$$

7.4 Consequences for Quantum Walks

The index theory of projections helps us to make statements for quantum walks analogous to the case of quantum cellular automata, i.e., we find a theorem for quantum walks corresponding to Theorem 3.7. The main difference, compared to the QCA case, is that the index for quantum walks is additive under multiplication or composition of walks and not multiplicative. But this is only due to the natural definitions and not of fundamental interest, because an "exponentiated" or "logarithmized" version of one of the indices would do the same job. Note that the composition of two independent quantum walks is given by a direct sum

structure, whereas the composition of independent quantum cellular automata was defined by a tensor product.

The results follow almost immediately from the general theory of the previous Section, just by specifying that the two projections are connected by a local unitary. Nevertheless, we find the following Main Theorem:

Theorem 7.8 *Let P be the projection onto $\bigoplus_{x\geq 0}\mathcal{H}_x$ and $\operatorname{ind} U = \operatorname{tr}(P - U^*PU)$ for any local unitary U. Then we have:*

(*i*) $\operatorname{ind} U$ *is an integer for any local unitary* U.

(*ii*) *The index is unchanged if we replace the projection P by any other projection onto a positive half-axis.*

(*iii*) $\operatorname{ind}(U_1 \oplus U_2) = \operatorname{ind} U_1 + \operatorname{ind} U_2$ *for the walk $U_1 \oplus U_2$ on the Hilbert space with $\mathcal{H}_x = \mathcal{H}_x^{(1)} \oplus \mathcal{H}_x^{(2)}$.*

(*iv*) $\operatorname{ind}(U_1U_2) = \operatorname{ind} U_1 + \operatorname{ind} U_2$ *for walks U_1, U_2 on the same Hilbert space and* $\operatorname{ind}(S^x) = x \dim \mathcal{H}_0$.

(*v*) *There exists a local decoupling for U, i.e. an operator V with $[P, UV] = 0$, which acts like the identity on all but finitely many $\mathcal{H}_x$, if and only if* $\operatorname{ind} U = 0$. *In detail, the decoupling V can be chosen such that it is equal to the identity on all subspaces $\mathcal{H}_x$ with $x < -L$ and $x \geq L$, if L is the width of U.*

(*vi*) $\operatorname{ind} U = 0$ *if and only if U can be locally deformed to the identity, i.e. there exists a norm continuous path $[0,1] \ni t \mapsto U_t$ of local unitaries of width $4L-1$ such that $U_0 = U$ and $U_1 = \mathbb{1}$.*

Proof:

(*i*) Follows directly from Theorem 7.7.

(*ii*) Let $\tilde{P}$ be a projection onto another positive half-axis. Then $P - \tilde{P}$ is a finite rank operator and hence $(P - U^*PU) - (\tilde{P} - U^*\tilde{P}U) = P - \tilde{P} - U^*(P - \tilde{P})U$ is the difference of two finite rank operators with equal trace.

(*iii*) Follows directly from the trace formula and $P = P^{(1)} \oplus P^{(2)}$.

(*iv*) The index of the shift follows directly from the definition, e.g. Eq. (7.6). The sum formula is due to $P - U_2^*U_1^*PU_1U_2 = (P - U_2^*PU_2) + U_2^*(P - U_1^*PU_1)U_2$ and Proposition 7.3.

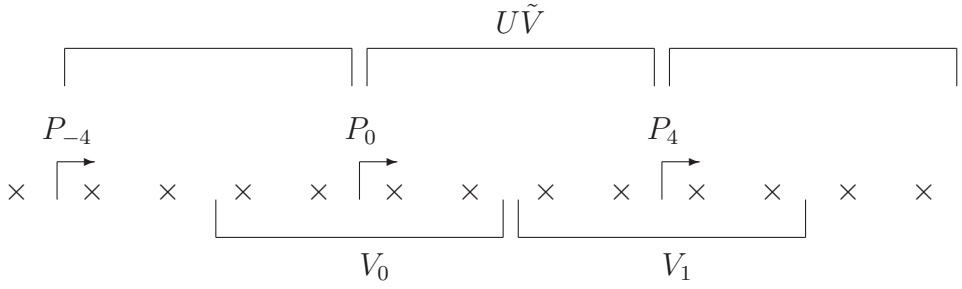

Figure 7.1: *Contraction of a walk of width $L = 2$ to the identity.*

(*v*) Apply Theorem 7.4 to get V with $P = V^*U^*PUV$. Since U is local, the difference $P - U^*PU$ vanishes on all subspaces $\mathcal{H}_x$ with $x \geq L$ and $x < -L$. In particular, both operators P and U^*PU act like the identity for $x \geq L$ and vanish for $x < -L$. Therefore, the space $\mathcal{H}_{(L)} := \bigoplus_{x<-L, x\geq L} \mathcal{H}_x$ has no overlapp with $\ker(P - U^*PU \pm \mathbb{1})$ and, by looking at the proof of Thm. 7.4, we have $V|_{\mathcal{H}_{(L)}} = |\mathbb{1} - P - U^*PU|^{-1}(\mathbb{1} - P - U^*PU)|_{\mathcal{H}_{(L)}} = \mathbb{1}_{\mathcal{H}_{(L)}}$.

(*vi*) Carry out the decoupling construction for all projections P_{2kL} onto the half axes $x \geq 2kL$. According to the previous part, the different decoupling unitaries V_k do not overlapp and their direct sum, denoted by $\tilde{V}$ is a local unitary of width $2L - 1$. By contracting each of the V_k to $\mathbb{1}$, this $\tilde{V}$ can be continuously deformed to the identity. $U\tilde{V}$ is then block diagonal with respect to the intervals $x \in \{2kL, \ldots, 2(k+1)L - 1\}$, i.e. a local unitary of width $2L - 1$. This operation can also be contracted to the identity and altogether this gives a path of local unitaries of maximal width of $4L - 1 = 2 \times \text{width}(U\tilde{V}) + 1$ (see Figure 7.1 for the case $L = 2$).

■

Note that (*i*) and (*iv*) imply that the index is a homomorphism from the multiplicative group of local unitaries into the additive group of integers. As in the case of QCAs, all possible indices can be represented by shift operations. Especially, every local unitary can be transferred to one with trivial index by multiplying with a conditional shift.

7.5 Translationally Invariant Case

In Chapter 6 we have already considered the structure of translationally invariant quantum walks. To remind you of, these are best described in momentum space,

i.e., by a unitary matrix

$$\hat{U}(p) = \sum_{x=-L}^{L} U_x e^{ipx}\,, \tag{7.20}$$

when U_x are constant $d \times d$-matrices and L the width of the walk[1]. Note that we do not flatten the internal structure in this case, i.e., we assume that $\mathcal{H}_x \cong \mathbb{C}^d$ holds for all $x \in \mathbb{Z}$. The matrix elements of $\hat{U}(p)$ are Laurent-polynomials in the variable e^{ip}, and in Lemma 6.1 we observed that the determinant of $\hat{U}(p)$ is a monomial. The exponent of this monomial was denoted by the index of the walk. The following Proposition states that this is indeed in accordance to the general definition of the index.

Proposition 7.9

(*i*) *Let U be a translationally invariant walk with* $\det \hat{U}(p) = \phi\, e^{inp}$. *Then we have*

$$\operatorname{ind} U = n\,. \tag{7.21}$$

(*ii*) *Let U be a translationally invariant walk with* $\operatorname{ind}(U) = 0$. *Then we can find a norm continuous path $t \mapsto U_t$ of translationally invariant walks of bounded width with $U_0 = \mathbb{1}$ and $U_1 = U$.*

Proof:

(*i*) With the factorization of Prop. 6.2 the walk decomposes into constant unitaries, which do not contribute to the index, and conditional shift operations $\tilde{S}_k(p) = \operatorname{diag}(e^{ikp}, 1, \ldots, 1)$. By (*ii*) of Theorem 7.8 $\operatorname{ind}(\tilde{S}_k) = k$ holds, and by calculating the determinant $n = \sum k$. With the product formula for the index ((*iii*) of Theorem 7.8) the result follows.

(*ii*) We use the same factorization as in the previous case. The width of U is bounded by $L_{max} = \sum_{k>0} k$ and the walk can be deformed to the identity by contracting all the constant unitaries to $\mathbb{1}$. The width of all U_t is then clearly bounded by L_{max}.

■

The determinant formula shows that the index only depends on the eigenvalues $e^{i\omega_1(p)}, \ldots, e^{i\omega_d(p)}$ of $\hat{U}(p)$. In particular, we get

$$\sum_{k=1}^{d} \omega_k(p) \,(\mathrm{mod}\, 2\pi) = p \operatorname{ind} U\,,$$

[1]Note that in Chapter 6 we did not use a symmetric neighborhood and we denoted by L the length of the unitary.

and by differentiating

$$\sum_{k=1}^{d} \frac{d\omega_k}{dp} = \operatorname{ind} U \,. \tag{7.22}$$

These relation helps us to connect the index with the group velocity operator

$$V(p) = -i\hat{U}(p)^* \frac{d}{dp}\hat{U}(p)\,, \tag{7.23}$$

which was introduced in Section 2.3 by Eq. (2.25). Let $W(p)$ be the unitary with $W(p)^*\hat{U}(p)W(p) = \operatorname{diag}(e^{i\omega_1(p)}, \ldots, e^{i\omega_d(p)})$. Then with

$$0 = \frac{d}{dp}\mathbb{1} = \frac{d}{dp}(W(p)W(p)^*) = \left(\frac{d}{dp}W(p)\right) W(p)^* + W(p)\frac{d}{dp}W(p)^*$$

it is easy to see that

$$\operatorname{tr} V(p) = \sum_{k=1}^{d} \frac{d\omega_k}{dp} \tag{7.24}$$

holds. Furthermore, we have

$$\begin{aligned} \operatorname{ind} U &= \frac{1}{2\pi i}\int_{-\pi}^{\pi} dp\, \operatorname{tr}\left(\hat{U}(p)^*\frac{d}{dp}\hat{U}(p)\right) && (7.25)\\ &= d\operatorname{tr}(\rho V) && (7.26) \end{aligned}$$

where ρ is an initial state which is localized at position $x = 0$, but totally mixed in the coin space, i.e. $\frac{1}{d}\mathbb{1}_d$. This implies that the index is connected to the mean group velocity, i.e., up to a factor d the index is given by the expectation value of the velocity operator, averaged over the coin space. This was already observed by Kitaev [Kit05], but we also find the following Proposition.

Proposition 7.10 *Let U be a translationally invariant walk and $e^{i\omega_1(p)}, \ldots, e^{i\omega_d(p)}$ the eigenvalues of $\hat{U}(p)$. Then the index of U is given by the winding number of the curve $\gamma : p \mapsto e^{i\sum_k \omega_k(p)}$.*

Proof: From Eq. (7.25) we find

$$\begin{aligned} \operatorname{ind} U &= \frac{1}{2\pi i}\int_{-\pi}^{\pi} dp\, e^{-i\sum_k \omega_k(p)}\frac{d}{dp}e^{i\sum_k \omega_k(p)}\\ &= \frac{1}{2\pi i}\int_{\gamma}\frac{dz}{z}\,, \end{aligned}$$

which is exactly the winding number of γ. ■

This Proposition enables us, to read the index off the diagram of the dispersion relation ω_k, i.e., the index is given by the signed number of crossings of any horizontal line (compare Fig. 7.3).

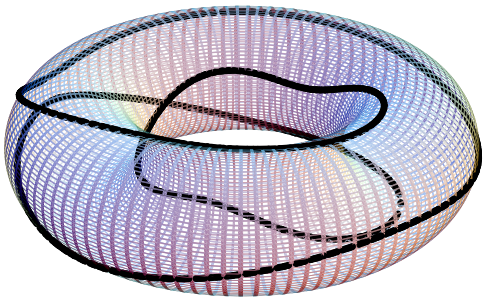

Figure 7.2: *Eigenvalues of $\hat{U}(p)$ from Example 7.11 as they wind around the torus. In this case we get a single curve.*

Example 7.11 Let us consider the quantum walk

$$\hat{U}(p) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & & \\ & 0 & 1 \\ & 1 & 0 \end{pmatrix} \begin{pmatrix} e^{ip} & & \\ & 1 & \\ & & e^{ip} \end{pmatrix} V^T \begin{pmatrix} e^{-ip} & & \\ & e^{-ip} & \\ & & e^{ip} \end{pmatrix} \begin{pmatrix} 1 & & 1 \\ & \sqrt{2} & \\ 1 & & -1 \end{pmatrix} \begin{pmatrix} 1 & & \\ & e^{ip} & \\ & & e^{-ip} \end{pmatrix} V$$

with

$$V = \frac{1}{\sqrt{6}} \begin{pmatrix} \sqrt{2} & \sqrt{3} & 1 \\ \sqrt{2} & -\sqrt{3} & 1 \\ -\sqrt{2} & 0 & 2 \end{pmatrix},$$

i.e., we have $d = 3$, $L = 2$ and $\mathrm{ind}(U) = 1$. The eigenvalues winding around the torus are displayed in Fig. 7.2, the dispersion relations are shown in Fig. 7.3. ◊

7.5.1 Higher Lattice Dimensions

As already mentioned in the case of quantum cellular automata, a generalization of the index theory to higher lattice dimensions is much more promising in the translationally invariant case, simply because without translation symmetry there is too much freedom for information flow in the system. Nevertheless, for QCAs we are only able to tackle some special cases, but here we show that for quantum walks most results can be generalized to higher lattice dimensions.

The most important observation for doing this was already described in the previous Chapter. In Lemma 6.1 we have seen that the determinant of the Fourier transform $\hat{U}(p_1, \ldots, p_s)$ of a walk U is always a monomial. In the one-dimensional

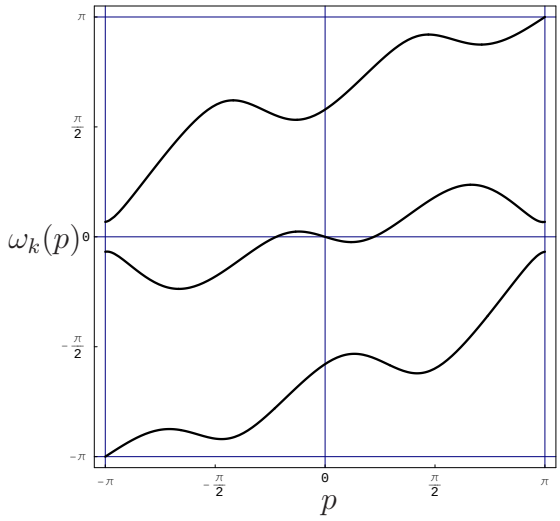

Figure 7.3: *Dispersion relation of $\hat{U}(p)$ from Example 7.11. With Eq. (7.22) the index can be computed by the sum of the derivatives of all branches, or with Prop. 7.10 by the signed number of crossing of any horizontal line.*

case we found that the index of U is given by the exponent of this monomial, which gives rise to the following Definition.

Definition 7.12 *Let U be a translationally invariant quantum walk on the lattice $\mathbb{Z}^s$ with Fourier transform $\hat{U}(p_1, \ldots, p_s)$. Let $\det \hat{U} = \phi \exp(i \sum_j n_j p_j)$ according to Lemma 6.1. Then the index of U is defined by*

$$\operatorname{ind} U = (n_1, \ldots, n_s)\,, \tag{7.27}$$

i.e. by a tuple of s integer numbers $n_1, \ldots, n_s$.

In particular, the index assigns an integer number to the walk for each lattice direction. These numbers are related to the indices of one-dimensional walks in the following way: From a s-dimensional walk we construct a one-dimensional walk $U^{(j)}$ in lattice direction j by making periodic boundary conditions in all other directions. The index of $U^{(j)}$, normalized with the length of the boundary conditions, is then given by n_j, i.e. by the jth component of $\operatorname{ind} U$.

Of course, one would also like to establish results corresponding to the Main Theorem 7.8 for the one-dimensional case. But most of the points are easily checked:

(i) In this case the index is by definition a tuple of integers.

(ii) Considering the trace formula makes only sense when the walk is reduced by periodic boundaries to a one-dimensional one, and then the statement is trivially true from the one-dimensional case.

(*iii*) $\mathrm{ind}(U_1 \oplus U_2) = \mathrm{ind}\, U_1 + \mathrm{ind}\, U_2$ holds, because the determinant of a direct sum gives the product of the determinants.

(*iv*) $\mathrm{ind}(U_1 U_2) = \mathrm{ind}\, U_1 + \mathrm{ind}\, U_2$ holds with $\det(AB) = \det(A)\det(B)$. For a shift $S^{(j)}$ in lattice direction j we have $(\mathrm{ind}\, S^{(j)})_i = \delta_{ij}$.

(*v*) As in (*ii*) a local decoupling makes only sense by reducing to one dimension.

(*vi*) The deformation to the identity is an open problem since a factorization into shift steps and one-site rotations seems not possible in general. However, more abstract theories like coarse geometry and K-theory may help at this point [Roe03, Roe96].

7.6 Conclusions

We have introduced an index theory for local unitaries transforming single particles or excitations, which are distributed over a one-dimensional lattice, i.e., unitaries on Hilbert spaces of the form $\bigoplus_{x=-\infty}^{\infty} \mathcal{H}_x$, where all $\mathcal{H}_x$ are finite dimensional. In the translationally invariant case these local unitaries correspond exactly to the definition of quantum walks from the previous Chapter. The index is defined in terms of the information transfer between the left and the right half-axis, or equivalently, by the trace of the difference of a half-axis projection and its image under the local unitary. We have applied the powerful index theory for pairs of projections of Avron, Seiler and Simon [ASS94b] to our case. We found that the index is in any case an integer number which does not depend on the intersection point, i.e. on which positive half-axis we have chosen, even when we do not assume that the local unitaries are translationally invariant. This means that similar to the case of quantum cellular automata (compare Chapter 3) the index is a local computable quantity which is constant along the line. We have also shown that the index (as a map) is additive under multiplication and composition of local unitaries, which means that it is a homomorphism from the group of local unitaries into the additive group of integers. Analogously to the case of quantum cellular automata, we have shown that the local unitaries with trivial index are exactly those, which can be locally decoupled and locally deformed to the identity.

In the translationally invariant case, i.e. in the case of the previous definition of quantum walks, we also established that the index is, up to the dimension of a single Hilbert space, equal to the mean group velocity of the system, i.e. the expectation values of the velocity operator averaged over all single-site input states. Furthermore, the index is equal to the winding number of the eigenvalues of the quantum walk in momentum space. In the translationally invariant case we have also generalized most results to higher lattice dimensions.

Chapter 8

Decoherent Quantum Walks

In this Chapter we study quantum walks with experimental imperfections. We characterize the structure of Kraus operators, which lead to local and translationally invariant, but irreversible dynamics. For any given set of Kraus operators we answer whether the propagation behavior is ballistic as in the undisturbed quantum case or diffusive as in the classical case. In particular, we find that such a quantum to classical transition happens in the case of random unitary evolutions. We also show how to compute the variance of the probability distribution analytically. As a realistic noise model we introduce a quantum walk with fluctuating coin parameters and calculate the variance of the distribution for this model. We also find that for many decoherence models the first order disturbance process is described by a loss of information in the internal degree of freedom.

The results of this Chapter are joint work with Annette Gattner.

8.1 Introduction

Every experimental realization of a quantum walk is influenced by some kind of error. For instance, with some small probability the implemented coin operation differs a little bit from the desired one. To detect decoherence sources in an experiment is the first step for improving the fidelity of the experiment. Hence, it is important to understand, how the probability distribution is influenced by certain dissipation processes and to model realistic experimental imperfections.

Since every experimental implementation is disturbed by dissipation, it is not surprising that there exist already several papers concerning decoherent quantum walks. Most of them present numerical results for special kinds of errors such as in [DRKB02], where experimental imperfections are discussed after the presentation of a proposal for an experimental realization. Numerical results are shown for the depolarizing channel, phase errors in the coin degree of freedom and incoherent tunneling. In [LP03], the coupling to an environment is modeled by

random coin rotations. In [SBBH03], unitary noise is studied numerically. Unitary noise means that the given unitary quantum walk is rotated by a stochastic unitary operator in every time step. It is worth mentioning that in all papers containing numerics, these are very well elaborated, i.e., a lot of time steps can be simulated. In the last one mentioned, simulations are shown up to 10000 time steps.

Analytical results for the long time behavior can also be found, but general statements are never made since just special examples of decoherence are considered. In [KT02, KT03a, KT03b] projections onto the coin as well as the position degree of freedom performed after the unitary walk with a small probability q are considered, and the variance is calculated for large times T, more precisely for $T \gg 1$ AND $qT \ll 1$. In [BCA03a, BCA03b] the authors achieve a lot by calculating the first two moments in momentum space. It is, however, necessary to specify the decoherence to be able to make statements on the long time behavior. They consider pure dephasing. The same method is used in [ADSS07] to study bit-flip channel noise and randomly broken links. In [RSA$^+$05], periodic measurements on both degrees of freedom are studied analytically and numerical results for a quantum walk with broken links are presented. In [KBH06], it is shown that the quantum walk with generalized Grover coin and random phase shifts in each time step shows diffusive propagation behavior. In [Zha08] the limit distributions of the Hadamard walk, which is disturbed by measurements on both degrees of freedom, are shown to be gaussian for certain initial states. Such a quantum to classical transition was observed in all the papers mentioned here. An overview can be found in [Ken06].

As mentioned in the previous chapters, quantum walks are not defined by a direct quantization of random walks because an internal degree of freedom has to be introduced. However, the behavior of quantum walks under decoherence shows that random walks indeed correspond to the classical processes. Note that a quantum to classical transition can also be found in unitary quantum walks driven by many coins [BCA03c, SK08].

8.1.1 Outlook and Summary of Results

In the following Section we study the structure of general decoherent quantum walks, i.e. completely positive maps on $\ell^2(\mathbb{Z}^s) \otimes \mathbb{C}^d$, which are local and translationally invariant. We find that the Kraus operators may contain momentum shifts, i.e., they are not necessary translationally invariant. In Section 8.3 we consider the asymptotic behavior of decoherent quantum walks. In particular, we use perturbation theory techniques to decide for any given set of Kraus operators, whether the propagation is diffusive or ballistic. We distinguish the analysis between commuting and non-commuting Kraus operators, where we do not assume momentum shifts at first. These are considered by example in Subsection 8.3.5. In Subsection 8.3.4 we introduce a model with fluctuating coin parameters and

we compute the variance of the probability distribution in dependence of the diffusion constant of the coin parameter. In Section 8.4 we show that for most decoherence processes the first order process is loosing the information about the coin state, which then leads to diffusive behavior.

8.2 General Structure

To model a non-unitary evolution without the loss of particles, we have to consider maps which map density operators to density operators. This condition is guaranteed by completely positive maps, so called channels, which can be written explicitly in the Kraus representation (see Proposition 2.3)

$$W(\rho) = \sum_{j=1}^{m} K_j \, \rho K_j^* \, . \tag{8.1}$$

The basic idea is to let the first Kraus operator be the given, but now disturbed quantum walk which happens with a certain probability, and the other Kraus operators the decoherent effects. For instance, they can model the use of another coin, phase rotations or shift errors. Since we do not want to lose our single particle, we require the Kraus operators K_j to fulfill the normalization condition $\sum_{j=1}^{m} K_j^* K_j = \mathbb{1}$ and, to prevent the walk from spreading out arbitrarily fast, to fulfill the locality condition introduced in the previous chapters.

To determine the general structure of translationally invariant quantum walks, we have to study this invariance on a larger Hilbert space given by the Stinespring dilation (Theorem 2.2). The time evolution is then given by an isometry $\mathcal{V} : \mathcal{H} \to \mathcal{H} \otimes \mathcal{K}$ with $\mathcal{V}^*\mathcal{V} = \mathbb{1}$, $\mathcal{H} = \ell^2(\mathbb{Z}^s) \otimes \mathbb{C}^d$, the dilation Hilbert space $\mathcal{K}$ and:

$$W(\rho) = \mathrm{tr}_{\mathcal{K}} \left(\mathcal{V} \rho \mathcal{V}^* \right) \, . \tag{8.2}$$

If $\psi, \phi \in \mathcal{H}$ and $\sum_j |e_j\rangle\langle e_j| = \mathbb{1}_{\mathcal{K}}$ holds, the Kraus and the Stinespring operators are related as follows: $\langle \psi, K_j \, \phi \rangle = \langle \psi \otimes e_j, \mathcal{V} \, \phi \rangle$. It is not necessary that the $\{|e_j\rangle\}$ form a basis, but, for the following considerations, we want them to be one. Moreover, due to reasons of lucidity, the following considerations are made in just one lattice dimension, but the argumentation holds also for arbitrary lattice dimensions and can easily be extended, similar to the asymptotic behavior of unitary walks.

Proposition 8.1 *A general translationally invariant quantum walk in position space is given by the isometry*

$$\mathcal{V} : \quad \mathcal{H} \to \mathcal{H} \otimes \mathcal{K} \tag{8.3}$$

$$|x, \alpha\rangle \mapsto \sum_{a,\beta} |x + a, \beta\rangle \otimes \tilde{S}_x v_a(\alpha, \beta) \, , \tag{8.4}$$

with a position dependent phase $\tilde{S}_x = \sum_j e^{iq_j x}|e_j\rangle\langle e_j| \in \mathcal{B}(\mathcal{K})$*,* $v_a(\alpha,\beta) \in \mathcal{K}$ *and the normalization condition* $\delta_{xy}\delta_{\alpha\beta} = \sum_{a,\gamma}\langle \tilde{S}_{x-y}v_a(\alpha,\gamma), v_{a+x-y}(\beta,\gamma)\rangle$*.*

Remark By Fourier transformation, we obtain in momentum space

$$\hat{\mathcal{V}}|p,\alpha\rangle = \sum_{j,a,\beta} e^{-i(p+q_j)a}\ \langle e_j|v_a(\alpha,\beta)\rangle\ |p+q_j,\beta\rangle \otimes |e_j\rangle\,.$$

As expected, a position dependent phase multiplication in position space yields a momentum shift in momentum space. The Kraus operators are given by

$$K_j|p,\alpha\rangle = \sum_{a,\beta} e^{-i(p+q_j)a}\ \langle e_j|v_a(\alpha,\beta)\rangle\ |p+q_j,\beta\rangle\,. \tag{8.5}$$

Proof: A general map $\mathcal{V} : \mathcal{H} \to \mathcal{H}\otimes\mathcal{K}$ is given by $|x,\alpha\rangle \mapsto \sum_{a,\beta}|x+a,\beta\rangle \otimes v_a(\alpha,\beta,x)$ with $v_a(\alpha,\beta,x) \in \mathcal{K}$. Since we want the walk to be translationally invariant, we need $\mathcal{V}S_x = S_x \otimes \tilde{S}_x\mathcal{V}$, where S_x are space translations and $\tilde{S}_x$ are representations of . Since the walk has to fulfill the locality condition, we can choose $\dim\mathcal{K} < \infty$, what yields the expansion of $\tilde{S}_x = \sum_j e^{iq_j x}|e_j\rangle\langle e_j|$ in a basis. The intertwiner relation of $\mathcal{V}$ leads to $v_a(\alpha,\beta,x) = \tilde{S}_x v_a(\alpha,\beta,0) =: \tilde{S}_x v_a(\alpha,\beta)$, what yields the desired form. The normalization condition is a consequence of the isometry condition $\delta_{xy}\delta_{\alpha\beta} = \langle x,\alpha|\mathcal{V}^*\mathcal{V}|y,\beta\rangle$. ■

8.3 Asymptotic Behavior

We first consider quantum walks without momentum shifts because otherwise they are not easy to handle both in momentum and position space. In the following Subsection we describe the perturbation theory, which we will use to achieve our results. The perturbation theory suggests to study different cases, e.g. to distinguish whether the Kraus operators commute or not. In Subsection 8.3.4 we describe a model with fluctuating coin parameters and in Subsection 8.3.5 we consider an example with momentum shifts.

8.3.1 Perturbation Theory of the Long-Time Behavior

First, we assume that $\tilde{S}_x = \mathbb{1}$ (or $q_j = 0$) holds, i.e., the case without momentum shifts. The aim is to determine the scaling behavior of the position operator in the long time limit. As we have mentioned in Section 2.3, the propagation of the particle is diffusive in the classical case and ballistic in the unitary quantum case. In the presence of decoherence we therefore like to answer the question, whether $Q(t)/t$ as in the quantum case or $Q(t)/\sqrt{t}$ as in the classical case converges. To

do so, we study the time evolution of the exponential function $e^{i\lambda Q}$ which is given by

$$W(e^{i\lambda Q}) = \sum_{j=1}^{m} K_j^* \, e^{i\lambda Q} K_j \,, \tag{8.6}$$

and enables us to consider all moments of the position operator at once.

To obtain the desired limit in both cases, we first define the following function on arbitrary momentum dependent operators A

$$W_{\frac{\tilde{\lambda}}{t^\eta}}(A) := W(A\, e^{i\tilde{\lambda}Q/t^\eta}) \; e^{-i\tilde{\lambda}Q/t^\eta} \,. \tag{8.7}$$

Hence, the desired limit can be obtained by considering $W^t_{\frac{\tilde{\lambda}}{t^\eta}}(\mathbb{1}) \;\; e^{i\tilde{\lambda}Q/t^\eta}$ and determining the scaling behavior given by η. For simplicity, we set $\lambda = \tilde{\lambda}/t^\eta$ for the next few steps and keep in mind that it is small for large times. It is easy to see that the defined function is translationally invariant since $W_\lambda(e^{iP}Ae^{-iP}) = W(e^{iP}A\, e^{-iP}e^{i\lambda Q}) \; e^{-i\lambda Q} = e^{iP} \; W(A\, e^{i\lambda Q})\, e^{-i\lambda}e^{-iP}e^{-i\lambda Q} = e^{iP}W_\lambda(A)e^{-iP}$ holds, where the commutation relation $[P,Q] = -i\mathbb{1}$ has been used, and we have that $W^t_\lambda(A) = W^t(A\, e^{i\lambda Q}) \; e^{-i\lambda Q}$.

Since W_λ is translationally invariant, all eigenoperators will commute with the momentum operator, i.e., they can be described by momentum dependent matrices in the form $(A\psi)(p) = A(p)\psi(p)$. Regarding that the two exponential functions in (8.7) are nothing else than a momentum shift, the action of W_λ on this kind of operators is given by

$$W_\lambda(A)(p) = \sum_{j=1}^{m} K_j^*(p)\, A(p)\, K_j(p+\lambda) \,. \tag{8.8}$$

Since λ is small, we can consider it as a small perturbation and, thus, have to do perturbation theory. This means that we have to find the eigenvalues and eigenoperators of the disturbed eigenvalue equation

$$W_\lambda(A_\lambda) = \mu_\lambda A_\lambda \,. \tag{8.9}$$

To do this, we first expand the eigenvalues and eigenoperators in demand and the Kraus operators up to the second order in λ:

$$A_\lambda = A + \lambda A' + \frac{\lambda^2}{2} A'' + \cdots \,, \tag{8.10}$$

$$\mu_\lambda = 1 + i\lambda\mu' - \frac{\lambda^2}{2} \mu'' + \cdots \,, \tag{8.11}$$

$$K_j(p+\lambda) = K_j(p) + \lambda K_j'(p) + \frac{\lambda^2}{2} K_j''(p) + \cdots \,, \tag{8.12}$$

where A are the eigenoperators of the undisturbed eigenvalue equation to the eigenvalue one.

Two cases have now to be distinguished: If there are degenerated eigenvalues for the undisturbed problem, the correct eigenbasis must be chosen, if not, the eigenvalue and the eigenoperators can be simply determined for the small parameter λ by inserting the expansions into the eigenvalue equation. The first case is equivalent to the case of commuting Kraus operators.

8.3.2 Commuting Kraus Operators

Theorem 8.2 *Let all the Kraus operators commute, such that they can be expanded in a common eigenbasis: $K_j(p) = \sqrt{q_j} \sum_\alpha e^{i\,\omega_{j,\,\alpha}(p)}\, P_\alpha(p)$. Then, the long time behavior is given by*

$$\lim_{t\to\infty} W^t\left(e^{i\lambda Q/t}\right)(p) \;=\; \sum_\alpha e^{i\lambda \sum_j q_j \,\frac{\partial \omega_{j,\,\alpha}(p)}{\partial p}}\, P_\alpha(p) = e^{i\lambda \sum_j \, q_j\, V_j(p)}\,, \quad (8.13)$$

where $V_j(p)$ is the velocity operator of the Kraus operator $\frac{1}{\sqrt{q_j}} K_j(p)$ as given in Eq. (2.25).

Proof: The Theorem coincides with the case of degenerated eigenvalues. If we just have one Kraus operator which then has to be unitary, or if all the Kraus operators commute, we can choose a common eigenbasis $|\psi_\alpha(p)\rangle$ $(\alpha = 1, \ldots, d)$ in which all the operators can be expanded: $K_j(p) = \sqrt{q_j} \sum_\alpha e^{i\,\omega_{j,\,\alpha}(p)}\, |\psi_\alpha(p)\rangle\langle\psi_\alpha(p)|$. It is easy to see that all the $|\psi_\alpha(p)\rangle\langle\psi_\beta(p)|$ are eigenoperators of the undisturbed problem, but only the projectors $P_\alpha(p) = |\psi_\alpha(p)\rangle\langle\psi_\alpha(p)|$ are eigenoperators to the eigenvalue 1. Thus, this eigenvalue is degenerated and, since we are interested in $W_\lambda(\mathbb{1}) = \sum_\alpha W_\lambda(P_\alpha)$ for small λ, this is the only interesting eigenvalue in this case.

By inserting the expansions mentioned above into the eigenvalue equation (8.9) for an eigenoperator $A_\alpha = P_\alpha$, we obtain for the first order of λ

$$W(A'_\alpha) - A'_\alpha = i\mu'_\alpha P_\alpha - \sum_{j=1}^{m} K_j^* P_\alpha\, K'_j\,. \quad (8.14)$$

Taking the trace and including that the quantum walk is trace invariant and $\mathrm{tr}\,(P_\alpha) = 1$, we obtain

$$\mu'_\alpha \;=\; -i\,\mathrm{tr}\left(\sum_{j=1}^{m} K_j^*(p) P_\alpha(p)\, K'_j(p)\right)$$

$$= -i \sum_{j=1}^{m} \mathrm{tr}\Bigg(q_j \sum_{\beta} e^{-i\omega_{j,\beta}(p)} P_\beta(p)\, P_\alpha(p) \cdot \sum_{\gamma} \left(i \frac{\partial \omega_{j,\gamma}(p)}{\partial p}\, e^{i\omega_{j,\gamma}(p)} P_\gamma(p) + e^{i\omega_{j,\gamma}(p)} \frac{\partial P_\gamma(p)}{\partial p} \right) \Bigg) .$$

Since the P_α are orthogonal projectors, we have $P_\alpha P_\beta = \delta_{\alpha\beta} P_\alpha$ and $P_\alpha \frac{\partial P_\gamma}{\partial p} P_\alpha = 0$, so we obtain

$$\mu'_\alpha = \sum_{j=1}^{m} \mathrm{tr}\left(q_j \frac{\partial \omega_{j,\alpha}(p)}{\partial p}\, P_\alpha(p) \right) = \sum_{j=1}^{m} q_j \frac{\partial \omega_{j,\alpha}(p)}{\partial p} ,$$

which coincides with a weighted addition of the momentum dependent velocities belonging to the eigenspace of P_α. This expansion can now be inserted into the function we want to determine:

$$\begin{aligned} W^t_{\frac{\tilde\lambda}{t}}(\mathbb{1})\; e^{i\tilde\lambda Q/t} &= \sum_\alpha W^t_{\frac{\tilde\lambda}{t}}(P_\alpha)\; e^{i\tilde\lambda Q/t} \\ &= \sum_\alpha \left(1 + i\frac{\tilde\lambda}{t} \sum_{j=1}^{m} q_j \frac{\partial \omega_{j,\alpha}(p)}{\partial p} + o\left(\frac{1}{t}\right) \right)^t P_\alpha(p)\; e^{i\tilde\lambda Q/t} , \end{aligned}$$

where $o\left(\frac{1}{t}\right)$ means that the rest contains only functions which decay faster than $1/t$. $\eta = 1$ was set, since a momentum dependent eigenvalue is already given by the first order of perturbation theory. By using Lemma B.2 and $\lim_{t\to\infty} e^{i\tilde\lambda Q/t} = \mathbb{1}$, we obtain

$$\begin{aligned} \lim_{t\to\infty} W^t\left(e^{i\tilde\lambda Q/t}\right)(p) &= \lim_{t\to\infty} W^t_{\frac{\tilde\lambda}{t}}(\mathbb{1})\; e^{i\tilde\lambda Q/t} \\ &= \sum_\alpha e^{i\sum_{j=1}^m q_j \frac{\partial \omega_{j,\alpha}(p)}{\partial p}} P_\alpha(p) \\ &= e^{i\sum_j\, q_j\, V_j(p)} , \end{aligned}$$

where V_j is the velocity operator as defined in Section 2.3 for the (normalized) Kraus operator $\frac{1}{\sqrt{q_j}} K_j$. ■

The Theorem tells us that, in the long time limit for commuting Kraus operators, it is possible to obtain a spread out proportional to the time t as well as a classical-like behavior if the velocity operator vanishes for all values of the momentum.

8.3.3 Non-commuting Kraus Operators

Theorem 8.3 *Let the Kraus operators not commute, such that there is no invariant subspace. Then, the long time behavior is given by*

$$\lim_{t\to\infty} W^t\left(e^{i\lambda Q/t}\right)(p) = e^{i\lambda\mu'(p)}\ \mathbb{1} \tag{8.15}$$

iff $\mu'(p) = -\frac{i}{d}\,\mathrm{tr}\left(\sum_{j=1}^m K_j^*(p)\,K_j'(p)\right)$ *is momentum dependent.*

It is given by

$$\lim_{t\to\infty} W^t\left(e^{(i\lambda Q-\lambda t\mu')/\sqrt{t}}\right)(p) = e^{-\lambda^2(\mu''(p)-\mu'^2)/2}\ \mathbb{1} \tag{8.16}$$

iff $d\,\mu' = -i\,\mathrm{tr}\left(\sum_{j=1}^m K_j^*(p)\,K_j'(p)\right) \in$ *is trivial, i.e., momentum independent. The behavior is then determined by the momentum dependent value* $\mu''(p) = -\frac{1}{d}\mathrm{tr}\left(\sum_{j=1}^m K_j^*(p)\,K_j''(p) + 2\sum_{j=1}^m K_j^*(p)A'\,K_j'(p)\right)$*. (*$A'$ *is specified in the proof.)*

Especially, in the case of random unitary operations we have the following behavior of the relevant functions.

Proposition 8.4 *If* $K_j^*K_j = K_jK_j^* \propto \mathbb{1}$ *holds for all* j*, then* $d\,\mu' \in$ *and* $\mu''(p) \geq 0$ *holds.*

Proof of Theorem 8.3: The Theorem corresponds to the case without degenerated eigenvalues. According to Lemma B.1 the only eigenoperator of the undisturbed problem to the eigenvalue 1 is $A = \mathbb{1}$: $W_{\lambda=0}(\mathbb{1}) = \sum_{j=1}^m K_j^*(p)\,\mathbb{1}\,K_j(p) = 1\cdot\mathbb{1}$. Thus, it is not degenerated. Moreover, we can set $\mathrm{tr}\,(A') = \mathrm{tr}\,(A'') = 0$ since the eigenoperators can be normalized such that $\mathrm{tr}(A_\lambda) = \mathrm{tr}(\mathbb{1}) = d$ holds for all λ.

By inserting these expansions into the eigenvalue equation (8.9), we obtain for the first order of λ

$$W(A') - A' = i\,\mu'\mathbb{1} - \sum_{j=1}^m K_j^*\,K_j'\,, \tag{8.17}$$

what enables us to calculate A' in every given case. Taking the trace and including that the quantum walk is trace invariant, we obtain

$$\mu' = -\frac{i}{d}\,\mathrm{tr}\left(\sum_{j=1}^m K_j^*(p)\,K_j'(p)\right)\,. \tag{8.18}$$

After differentiating the normalization condition $\sum_{j=1}^m K_j^*\,K_j = \mathbb{1}$, we see immediately that the real part of the trace above vanishes, such that μ' is real.

If μ' is momentum dependent, we obtain immediately using Lemma B.2 and the following convergence $\lim_{t\to\infty} e^{i\tilde{\lambda}Q/\sqrt{t}} = \mathbb{1}$:

$$\begin{aligned}\lim_{t\to\infty} W^t\left(e^{i(\tilde{\lambda}Q)/t}\right)(p) &= \lim_{t\to\infty} W^t_{\frac{\tilde{\lambda}}{t}}(\mathbb{1})\; e^{i\tilde{\lambda}Q/t} \\ &= \lim_{t\to\infty}\left(1+\frac{i\tilde{\lambda}\mu'(p)}{t}+o\left(\frac{1}{t}\right)\right)^t \mathbb{1}\; e^{i\tilde{\lambda}Q/t} \\ &= e^{i\tilde{\lambda}\mu'(p)}\;\mathbb{1}\,,\end{aligned}$$

If μ' is momentum independent, we have to consider the next order of perturbation theory: The second order in λ yields

$$W(A'') + 2\sum_{j=1}^m K_j^*\, A' K_j' + \sum_{j=1}^m K_j^*\, K_j'' = -\mu''\,\mathbb{1} + 2i\,\mu' A' + A''\,, \tag{8.19}$$

which leads to the momentum dependent value

$$\mu''(p) = -\frac{1}{d}\mathrm{tr}\left(2\sum_{j=1}^m K_j^*(p)\, A'(p) K_j'(p) + \sum_{j=1}^m K_j^*(p)\, K_j''(p)\right). \tag{8.20}$$

Now, the asymptotic distribution will be calculated. Since μ' is momentum independent, the whole probability distribution is shifted by exactly this value in every time step. The spread is thus determined by the second order of the perturbation calculation, because $\mu''(p)$ depends on the momentum, and is therefore diffusive, i.e., the spread is proportional to $\sqrt{t}$. We obtain for the long time behavior:

$$\begin{aligned}\lim_{t\to\infty} W^t\left(e^{i(\tilde{\lambda}Q-\tilde{\lambda}t\mu')/\sqrt{t}}\right)(p) &= \lim_{t\to\infty} W^t_{\frac{\tilde{\lambda}}{\sqrt{t}}}(\mathbb{1})\; e^{-i\tilde{\lambda}\mu'\sqrt{t}}\, e^{i\tilde{\lambda}Q/\sqrt{t}} \\ &= \lim_{t\to\infty}\left(1+\frac{i\tilde{\lambda}\mu'}{\sqrt{t}}-\frac{\tilde{\lambda}^2\mu''(p)}{2t}+o\left(\frac{1}{t}\right)\right)^t e^{-i\tilde{\lambda}\mu'\sqrt{t}}\,\mathbb{1}\, e^{i\tilde{\lambda}Q/\sqrt{t}} \\ &= e^{\tilde{\lambda}^2(\mu'^2-\mu''(p))/2}\;\mathbb{1}\,,\end{aligned}$$

where we have already removed the general shift by μ'. $o\left(\frac{1}{t}\right)$ means that the rest contains only functions which decay faster than $1/t$. In the last step, we have again used Lemma B.2 and the following convergence: $\lim_{t\to\infty} e^{i\tilde{\lambda}Q/\sqrt{t}} = \mathbb{1}$. ■

Proof of Proposition 8.4: To check that $d\,\mu'$ is a momentum independent value in , we use the factorization of every single unitary as introduced in Eq. (6.5). Inserting this factorization into the desired trace and using the property $\mathrm{tr}(XY) =$

$\mathrm{tr}(YX)$, one obtains $\mathrm{tr}\left(K_j^*(p)\,K_j'(p)\right) = i\,n_j$ for every unitary Kraus operator with index n_j, i.e.,

$$d\,\mu' = \sum_{j=1}^{m} n_j \quad \in \quad . \tag{8.21}$$

To show that $\mu''(p) \geq 0$, we again start considering only unitary Kraus operators and study the second term in the trace first. Inserting the factorization presented in Eq. (6.5), using $\mathrm{diag}(1,0,...,0)^2 = \mathrm{diag}(1,0,...,0)$, we obtain that the trace is of the form $-\mathrm{tr}\left(K_j^*(p)\,K_j''(p)\right) = \mathrm{tr}\,(X^*X) \geq 0$ for all j, since operators of the form X^*X are positive.

To be able to make statements on the first term, we first have to study A' more precisely. Due to Eq. (8.17) and $\partial_p \sum_{j=1}^m K_j^*\,K_j = 0$, we have that $A' + A'^* = W\,(A' + A'^*)$ has to hold. Lemma B.1 tells us know that $A' + A'^*$ has to be a scalar multiple of $\mathbb{1}$, but since $\mathrm{tr}A' = 0$ holds, we obtain that A' is a skew symmetric matrix, i.e., $A' = -A'^*$. Thus, A' has only imaginary eigenvalues and we can diagonalize it: $A' = iV^*DV$, with a unitary matrix V and a diagonal, real-valued matrix D. For each Kraus operator, we now obtain sums of terms of the form

$$\begin{aligned}
&-i\,\mathrm{tr}\left(\tilde{S}^*(p)W_k^*...\tilde{S}^*(p)W_1^*\;V^*DV\;W_1\tilde{S}(p)...W_k\tilde{S}(p)\;\mathrm{diag}(i,0,...,0)\right)\\
&\qquad = \mathrm{tr}\left(\tilde{S}^*(p)W_k^*...\tilde{S}^*(p)W_1^*\;V^*DV\;W_1\tilde{S}(p)...W_k\tilde{S}(p)\;\mathrm{diag}(1,0,...,0)\right)\\
&\qquad = \mathrm{tr}\Big(\mathrm{diag}(1,0,...,0)\tilde{S}^*(p)W_k^*...\tilde{S}^*(p)W_1^*\;V^*\sqrt{D}\\
&\qquad\qquad\qquad \cdot\sqrt{D}V\;W_1\tilde{S}(p)...W_k\tilde{S}(p)\;\mathrm{diag}(1,0,...,0)\Big)\,,
\end{aligned}$$

which is the trace of a positive operator. ■

In the long time limit for non commuting Kraus operators, both cases are in principal possible, i.e., there are both examples which show quantum-like behavior and examples of classical-like behavior. In the quantum-like case, the asymptotic probability is as in the unitary case given by the velocity distribution. In the classical-like case, the probability distribution converges to a gaussian distribution with variance $1/(\mu''(p) - \mu'^2)$ and expectation value μ' for every value of the momentum. Accordingly, Fourier transformation yields gaussian distributions with variance $\sigma(p)^2 = \mu''(p) - \mu'^2$, where σ is the standard deviation, in position space for every wave function concentrated around the momentum p. Moreover, the whole distribution is shifted by $t \cdot \mu'$ after t time steps. It should be stressed that this observation holds independent of the initial state since $\lim_{t\to\infty} \mathrm{tr}\left(\rho\,W^t\left(e^{i(\lambda Q - \lambda t\mu')/\sqrt{t}}\right)\right)(p) = e^{-\lambda^2(\mu''(p)-\mu'^2)/2}\;\mathrm{tr}\,(\rho\mathbb{1}) = e^{-\lambda^2\sigma(p)^2/2}$ for all values of momentum. The probability distribution spreads out with $\sqrt{t}$.

The Proposition states that this is always the case for random unitary operators, and $d\,\mu'$ is then a generalization of the index introduced in Chapter 6 to non-unitary walks. This case is studied numerically in Example 8.5.

Example 8.5 Let the Hadamard Walk be disturbed by a rotated coin, i.e., in every time step, the Hadamard Walk is implemented with probability $1-\epsilon$, but with probability ϵ the conditional shift is preceded by a rotated Hadamard coin:

$$W(\rho) = (1-\epsilon)\, U_H \rho\, U_H^* + \epsilon\, U_H U(\alpha) \rho\, U(\alpha)^* U_H^*\,, \tag{8.22}$$

$$\text{with} \quad U(\alpha) = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}. \tag{8.23}$$

This means that the walk is nearly not disturbed for small values of $\alpha \pmod{\pi}$. But, due to this small perturbation, it loses its ballistic behavior in the long time limit, i.e., the standard deviation σ becomes proportional to the square root of the time as in the classical case:

$$\mu' = 0 \tag{8.24}$$

$$\sigma(p)^2 = \mu''(p) - \mu'^2 = -1 + \frac{\cos\alpha}{(1-\epsilon)\sin\alpha} + \frac{1}{2\epsilon(1-\epsilon)\sin^2\alpha}\,, \tag{8.25}$$

which does not depend on the momentum in this case.

For $\alpha \to 0 \pmod{\pi}$ or $\epsilon \to 0$ or $\epsilon \to 1$, i.e., in the limits of no decoherence, the standard deviation diverges to infinity, since, in these cases, it does not scale with $\sqrt{t}$ but with t. This can be observed in the figures 8.1 and 8.2, where the position distribution after 50 time steps can also be found for several values of ϵ and α. For $\epsilon = 0.5$ and $\alpha = \pi/2$, the walk is the most achievable mixture of two quantum walks with two different coins, thus, the distribution is gaussian as in the classical case. For all other values of ϵ and α, the probability to move with maximal velocity has already decreased and the probability to be found at the origin which was also the initial position has already increased after 50 time steps. $\lozenge$

Remark The Theorems 8.2 and 8.3 characterize the asymptotic behavior of two extremal cases: All Kraus operators commute or the Kraus operators leave no subspace invariant. For these two cases the asymptotic behavior does not depend on the initial state (only the variance in the classical-like case may depend on the initial momentum distribution). In general one has to decompose the space into invariant subspaces and the asymptotic behavior has to be calculated for each subspace individually. Then it is possible that the asymptotic behavior depends on the initial state unless the asymptotic behavior is the same for all subspaces.

8.3.4 Fluctuating Coin Parameters

In this Subsection we want to make a first step to a realistic noise model of the quantum walk experiment in Bonn. In this experiment the coin parameters are

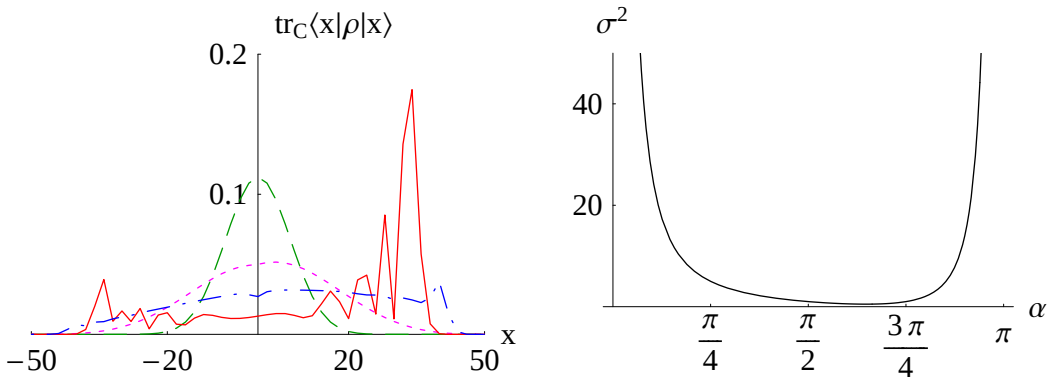

Figure 8.1: *Left: Probability distribution after 50 time steps for a particle, which started at the origin in the pure state* $\psi(x=0)=(1,0)^T$. *The parameters are* $\epsilon=0.5$ *for all lines,* $\alpha=0$ *for red drawn through line, i.e., this is the distribution of the undisturbed Hadamard walk,* $\alpha=\pi/2$ *for green dashed line,* $\alpha=\pi/8$ *for pink dotted line and* $\alpha=\pi/32$ *for blue dotted-dashed line. Right: Variance for* $q=0.5$ *dependent on the value of* α.

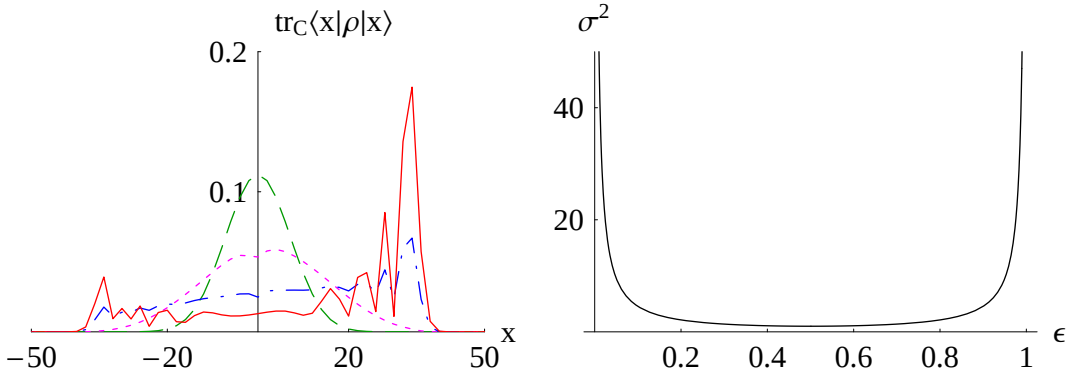

Figure 8.2: *Left: Probability distribution after 50 time steps for a particle, which started at the origin in the pure state* $\psi(x=0)=(1,0)^T$. *The parameters are* $\alpha=\pi/2$ *for all lines,* $\epsilon=0$ *for red drawn through line, i.e., this is the distribution of the undisturbed Hadamard walk,* $\epsilon=0.5$ *for green dashed line,* $\epsilon=0.1$ *for pink dotted line and* $\epsilon=0.02$ *for blue dotted-dashed line. Right: Variance for* $\alpha=\pi/2$ *dependent on the value of* ϵ.

adjusted by magnetic fields and, due to fluctuations of the magnetic field, the coin parameters are changed slightly in every time step [KFWM]. Therefore, we like to model a quantum walk with coin parameters which fluctuate in time. In particular, we want that the coin in time step $t+1$ differs only a little bit from the coin in time step t, i.e., the time evolution of the coin parameter can be modeled by a classical random walk.

The random walk of the coin parameter leads to a Gaussian distribution of the parameters, which is also used in the model of [SBBH03]. However, they use uncorrelated coin parameters, i.e., the parameters are chosen independently in each time step. They find that in this case the variance of the disturbed walk scales with the inverse of the variance of the parameter distribution.

The basic idea is to describe the coin parameter by an additional quantum state, which singles out the coin to be used, and to extend the dynamics by a random walk on this additional state. Thus, the total Hilbert space is given by $\mathcal{H} = \ell^2(\mathbb{Z}) \otimes \mathbb{C}^d \otimes \ell^2(\mathbb{Z})$. Let us first describe the dynamics of the additional system $\ell^2(\mathbb{Z})$. We denote the basis labels by $|c\rangle$ for $c \in \mathbb{Z}$ and in every timestep this label should increase or decrease, each with probability 1/2, i.e., the Kraus operators on this system are given by

$$\tilde{K_1}|c\rangle = \frac{1}{\sqrt{2}}|c+1\rangle\,, \quad \tilde{K_2}|c\rangle = \frac{1}{\sqrt{2}}|c-1\rangle\,. \tag{8.26}$$

The coin toss $U(c)$ should depend on the state of the additional system. The total coin toss acts therefore on $\mathbb{C}^d \otimes \ell^2(\mathbb{Z})$ and is given by

$$U = \sum_c U(c) \otimes |c\rangle\langle c|\,. \tag{8.27}$$

For this model, we assume that the shift operation is not disturbed, i.e., we will take a usual conditional shift S acting on $\ell^2(\mathbb{Z}) \otimes \mathbb{C}^d$. In total, we get for the quantum walk the following dynamics:

$$\begin{aligned} W(\rho) &= \sum_i (S \otimes \tilde{K_i})(\mathbb{1} \otimes U)\rho(\mathbb{1} \otimes U^*)(S^* \otimes \tilde{K_i}^*) \\ &= \sum_{i,b,c} (S \otimes \tilde{K_i})(\mathbb{1} \otimes U(c) \otimes |c\rangle\langle c|)\rho(\mathbb{1} \otimes U(b)^* \otimes |b\rangle\langle b|)(S^* \otimes \tilde{K_i}^*) \\ &= \frac{1}{2} \sum_{b,c,\alpha=\pm 1} S(\mathbb{1} \otimes U(c)) \otimes |c+\alpha\rangle\langle c|\rho(\mathbb{1} \otimes U(b)^*)S^* \otimes |b\rangle\langle b+\alpha|\,, \end{aligned}$$

the Kraus operators are thus given by

$$K_1 = \frac{1}{\sqrt{2}} \sum_c S(\mathbb{1} \otimes U(c)) \otimes |c+1\rangle\langle c|\,, \tag{8.28}$$

$$K_2 = \frac{1}{\sqrt{2}} \sum_c S(\mathbb{1} \otimes U(c)) \otimes |c-1\rangle\langle c|\,. \tag{8.29}$$

For a concrete example one only has to specify the coin $U(c)$ in dependence of the parameter c and the shift operation.

Example 8.6 Let us again consider the Hadamard walk, where the coin is rotated by an angle depending on c, e.g.

$$U(c) = \begin{pmatrix} \cos\frac{2\pi c}{n} & -\sin\frac{2\pi c}{n} \\ \sin\frac{2\pi c}{n} & \cos\frac{2\pi c}{n} \end{pmatrix} H\,, \tag{8.30}$$

where n is some fixed integer and H the Hadamard matrix. Obviously, the coin is periodic in c and therefore the additional space is effectively a random walk on a cycle with lattice constant $2\pi/n$. In particular, the additional Hilbert space is finite dimensional and isomorphic to $\mathbb{C}^n$. Starting from a fixed value, the variance of the coin parameter in dependence of the time is given by $(2\pi/n)^2 t$, i.e., the diffusion coefficient is $D(n) = 2\pi^2/n^2$ [Fel57]. Of course, we are interested in the less diffusive cases. Therefore we need to handle relatively large values of n.

In the case that n is even, there are some coins which commute. In particular, the set of coins is divided into $n/2$ pairs of commuting coins. Thus, there exist non-trivial operators commuting with the Kraus operators. Since we like to use the results of Theorem 8.3, we assume therefore that n is odd and we expect classical-like behavior. We want to compute the variance of the asymptotic position distribution with the techniques established in the previous sections. Thus, we have to calculate the first order perturbation of the eigenoperator $\mathbb{1}$ according to Eq. (8.17). In this case we have

$$K_j^*(p)K_j'(p) = \frac{1}{2}\sum_c U(c)^* \begin{pmatrix} i & \\ & -i \end{pmatrix} U(c) \otimes |c\rangle\langle c|\,, \tag{8.31}$$

and thereby $\mu' = -i/(2n)\sum_j \mathrm{tr}(K_j^*(p)K_j'(p)) = 0$. We then have to solve the equation

$$W(A') - A' + \sum_j K_j^*(p)K_j'(p) = 0\,. \tag{8.32}$$

Since the dimension of this space grows with n, we simplify the structure of the solution a little bit. Let $\phi, \psi \in \ell^2(\mathbb{Z}) \otimes \mathbb{C}^2$ be arbitrary and $|c\rangle, |\tilde{c}\rangle \in \mathbb{C}^n$ basis vectors. The equation $0 = \langle \phi \otimes c | W(A') - A' + \sum_j K_j^*(p)K_j'(p) | \psi \otimes \tilde{c}\rangle$ forces that $\langle \phi \otimes c | A' | \psi \otimes \tilde{c}\rangle = 0$ holds for $c \neq \tilde{c}$, i.e., A' is diagonal in the additional space. Therefore, A' can be expanded as

$$A' = \sum_c A'(c) \otimes |c\rangle\langle c|\,, \tag{8.33}$$

and Eq. (8.32) reduces to

$$A'(c) = U(c)^*\Big(1/2\, S^*(p)(A'(c+1) + A'(c-1))S(p) + \mathrm{diag}(i,-i)\Big)U(c) \tag{8.34}$$

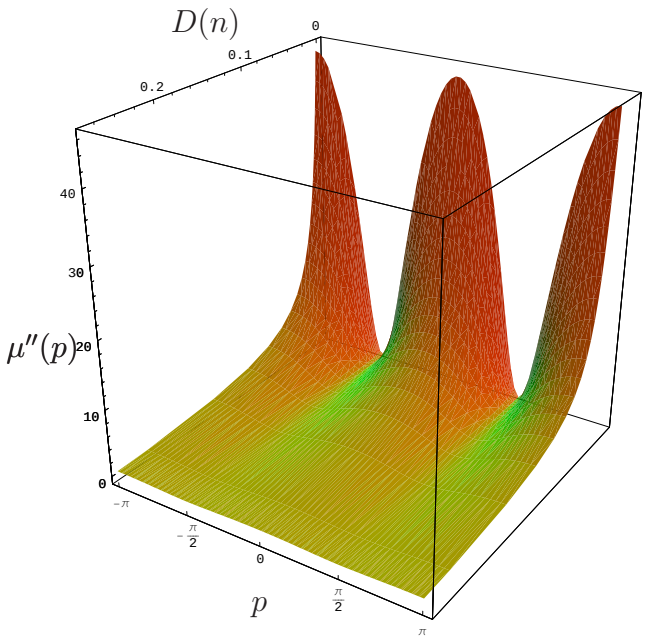

Figure 8.3: *Variance of the asymptotic distribution dependent on initial momentum and diffusion coefficient of the coin parameter.*

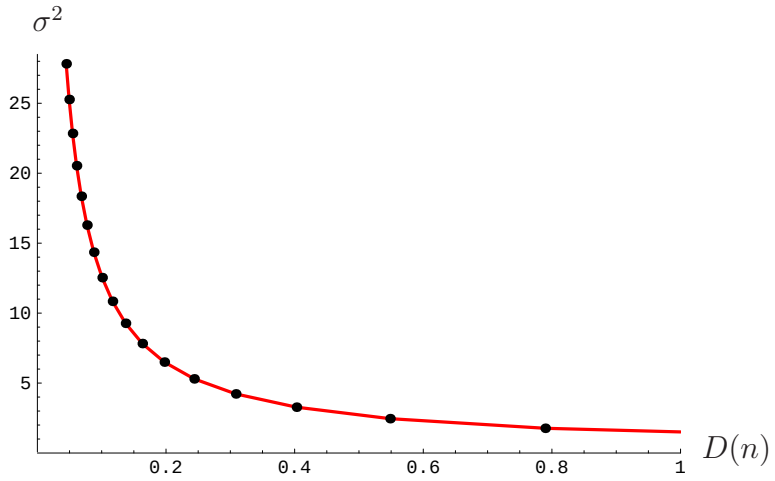

Figure 8.4: *Variance of the asymptotic distribution for a particle starting at the origin.*

for $c = 1, \ldots, n$. These equations can be solved numerically and the variance, which depends in this case on the momentum as illustrated in Figure 8.3, can be computed according to Eq. (8.20). For a particle initially located at a single site the variance, depicted in Figure 8.4, scales approximately as $1/D(n)$. $\Diamond$

8.3.5 Quantum Walks with Momentum Shifts

In the case of momentum shifts, or position dependent phases, we cannot make such a detailed characterization since it is not easy to deal with them both in momentum and in position space. But we can compare the behavior to the corresponding walk without momentum shifts for which we can characterize the asymptotic behavior according to the statements above. If the walk without momentum shifts shows quantum-like behavior, i.e. spreads out proportional to the time t, we get some kind of dispersion relation. The momentum shifts then lead to the effect that the velocity of the particle changes with each time step due to the momentum dependent dispersion relation. For long times the mean velocity will then be an average over the whole velocity range. This means the walk becomes diffusive, so the behavior turns classical-like. We will illustrate this effect by the following Example.

Example 8.7 Let us consider one lattice dimension with no internal degree of freedom, i.e., $\mathcal{H} = \ell^2(\ )$, and the following setting: $\dim \mathcal{K} = 2$, $q_1 = q_2 = q$, $v_{-1} = \frac{1}{2}\binom{0}{-1}$, $v_0 = \frac{1}{2}\binom{1}{1}$ and $v_{+1} = \frac{1}{2}\binom{1}{0}$. With $|e_1\rangle = \binom{1}{0}$ and $|e_2\rangle = \binom{0}{1}$, we obtain the Kraus operators

$$\begin{aligned} K_1|p\rangle &= \frac{1}{2}\left(1 + e^{ip}\right)|p+q\rangle \\ K_2|p\rangle &= \frac{1}{2}\left(1 - e^{-ip}\right)|p+q\rangle\,. \end{aligned}$$

Let us first assume the case without momentum shifts, i.e. $q = 0$. We have commuting Kraus operators, so according to Theorem 8.2 we have quantum-like behavior. The velocity operator is given by

$$V(p) = \lim_{t\to\infty} \frac{Q(t)}{t} = -i(K_1^* K_1' + K_2^* K_2') = \frac{1}{2}\cos(p)\,. \tag{8.35}$$

Remarkably, this is a quantum-like walk, although we have no internal degree of freedom, i.e., a system of which we know that there exists no non-trivial unitary quantum walk. This walk can therefore be interpreted as quantum walk with "classical coin toss".

In the case of a momentum shift the limit of $Q(t)/t$ will vanish because the average of the velocity is zero, and the asymptotic behavior turns classical-like. In figure 8.5 we have plotted for different values of q the probability distribution after 50 time steps. Only in the $q = 0$ case we have quantum-like behavior and

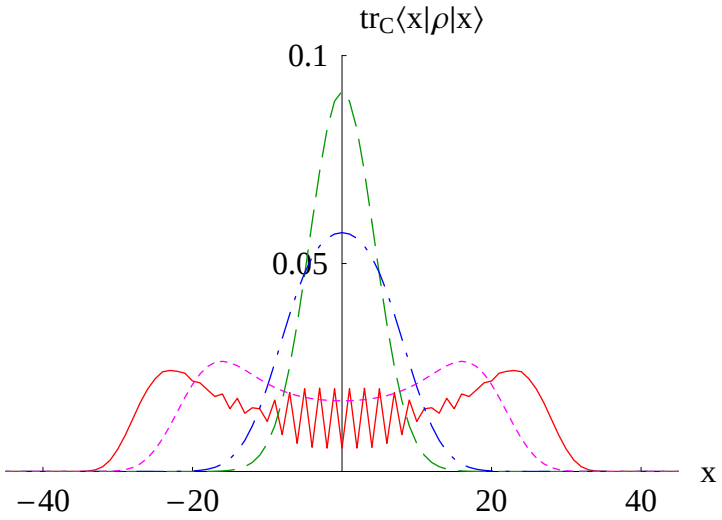

Figure 8.5: *Probability distribution for a particle which started at the origin in the pure state $\psi(x) = \delta_{x0}$ after 50 time steps. For $q = 0$ (red drawn through line) the behavior is quantum like, for $q = \pi/4$ (green dashed line) and $q = \pi/32$ (blue dotted-dashed line) the distribution looks already quite Gaussian. For $q = \pi/64$ (pink dotted line) the behavior looks still quantum-like, but after more time steps the distribution will also become Gaussian.*

for the larger values of q the distribution is already quite similar to a Gaussian distribution. ◊

8.4 Contraction Rates

We like to understand the process of decoherence in more detail. As argued in [ADSS07], the state reduced to the coin subspace converges towards a totally mixed state, i.e., the information about the internal degree of freedom is lost. Here we show that this process converges exponentially and we compute the contraction rate for the decoherent walk of Example 8.5 in dependence of the noise parameters.

First, suppose the quantum walk W fulfills

$$\left\| \mathrm{tr}_{\ell^2(\mathbb{Z})} W(\rho) - 1/d\, \mathbb{1} \right\| \leq \eta \left\| \mathrm{tr}_{\ell^2(\mathbb{Z})} \rho - 1/d\, \mathbb{1} \right\| \tag{8.36}$$

for all density operators ρ and some $\eta < 1$. Then we can conclude by a simple iteration that

$$\left\| \mathrm{tr}_{\ell^2(\mathbb{Z})} W^t(\rho) - 1/d\, \mathbb{1} \right\| \leq \eta^t \left\| \mathrm{tr}_{\ell^2(\mathbb{Z})} \rho - 1/d\, \mathbb{1} \right\| \tag{8.37}$$

holds, i.e. the operator $\mathrm{tr}_{\ell^2(\mathbb{Z})} W^t(\rho)$ converges exponentially fast to the maximally mixed state $1/d\, \mathbb{1}$. Hence, we only have to find a bound as in Eq. (8.36), which

we like to compute in momentum space. However, the operator $W(\rho)$ is not translationally invariant, i.e., it is of the general form $(A\psi)(p) = \int dk\, A(p,k)\psi(k)$. But for the partial trace over the spatial degree of freedom we have

$$\mathrm{tr}_{\ell^2(\mathbb{Z})} W(\rho) = \sum_{x\in\mathbb{Z}} W(\rho)(x,x) = \frac{1}{2\pi}\int_{-\pi}^{\pi} dp\, W(\rho)(p,p)\,.$$

Thus, we have for the norm distance from above

$$\left\|\mathrm{tr}_{\ell^2(\mathbb{Z})} W(\rho) - 1/d\,\mathbb{1}\right\| \leq \frac{1}{2\pi}\int_{-\pi}^{\pi} dp\, \left\|W(\rho)(p,p) - 1/d\,\mathbb{1}\right\|\,. \tag{8.38}$$

This means that we can bound the norm individually for all values of the momentum. One way of doing this is to consider the eigenvalues of W for the translationally invariant eigenoperators. Since $W(\mathbb{1}) = \mathbb{1}$ holds, at least one of the eigenvalues equals one, but this eigenvalue does not contribute to the norm distance. Suppose the second largest eigenvalue is $\eta < 1$. Then by decomposing ρ into eigenoperators of W, we find exactly the bound in Eq. (8.36). The eigenvalues can again be computed by perturbation theory as we will demonstrate in the following (similar techniques have been used in [TD00]).

We consider as in Subsection 8.3.3 non-commuting Kraus operators, where $\sqrt{1-\epsilon}U_1(p)$ describes the undisturbed problem and $\sqrt{\epsilon}U_2(p)$ the perturbation term, i.e. the decoherent quantum walk is in momentum space given by

$$W(A)(p,k) = (1-\epsilon)\, U_1(p)^* A(p,k) U_1(k) + \epsilon\, U_2(p)^* A(p,k) U_2(k)\,. \tag{8.39}$$

Consider for the unitary U_1 the spectral decomposition $U_1(p) = \sum_\alpha \omega_\alpha(p) P_\alpha(p)$ with the eigenprojectors $P_\alpha(p) = |\psi_\alpha(p)\rangle\langle\psi_\alpha(p)|$, where we assume that U_1 is non-degenerated ($\omega_\alpha(p) \neq \omega_\beta(p)$ for $\alpha \neq \beta$ and all values of p). Then the translationally invariant eigenoperators of W are given by $|\psi_\alpha(p)\rangle\langle\psi_\beta(p)|$ with eigenvalues $\overline{\omega_\alpha(p)}\omega_\beta(p)$. In this case we are doing first order perturbation theory, i.e., we compute the expectation values of the undisturbed eigenoperators in the presence of the perturbation terms. Note, however, that we have both the degenerated eigenvalue 1 (for every eigenoperator P_α) and the non-degenerate eigenvalues $\overline{\omega_\alpha(p)}\omega_\beta(p)$ for $\alpha \neq \beta$.

Let us first consider the non-degenerated part of the spectrum. We have (here we omit the dependence on p)

$$\mathrm{tr}\left(|\psi_\alpha\rangle\langle\psi_\beta| W(|\psi_\alpha\rangle\langle\psi_\beta|)\right) = \overline{\omega}_\alpha\omega_\beta(1-\epsilon\,(1-\langle\psi_\alpha|U_2|\psi_\alpha\rangle\langle\psi_\beta|U_2|\psi_\beta\rangle))\,. \tag{8.40}$$

For the degenerated part of the spectrum we consider the matrix

$$V_{\alpha\beta} = \mathrm{tr}(|\psi_\alpha\rangle\langle\psi_\alpha|(U_2^*|\psi_\beta\rangle\langle\psi_\beta|U_2 - \mathbb{1})) = |\langle\psi_\beta|U_2|\psi_\alpha\rangle|^2 - 1\,, \tag{8.41}$$

which eigenvalues then gives the correct perturbation terms. For getting the bound in Eq. (8.38) one has to integrate over the absolute value of the perturbed eigenvalues. The largest one of these (apart from eigenvalue 1) gives the desired bound.

Example 8.8 We consider again the decoherent quantum walk of Example 8.5 with the noise parameters ϵ, α. The two eigenvalues of the non-degenerate part have the same absolut value and integration over the momentum yields

$$\lambda_{12}(\epsilon, \alpha) = 1 + (\sqrt{2} - 2)\epsilon \sin(\alpha)^2 \,. \tag{8.42}$$

The eigenvalues of the degenerate part are $\lambda_2 = 1$ and

$$\lambda_1(\epsilon, \alpha) = 1 + 2(\sqrt{2} - 2)\epsilon \sin(\alpha)^2 \,. \tag{8.43}$$

In particular, λ_{12} (plotted in Figure 8.6) is larger than λ_1 for all values of ϵ and α and gives therefore the desired bound, i.e., we have

$$\left\| \mathrm{tr}_{\ell^2(\mathbb{Z})} W^t(\rho) - 1/d \, \mathbb{1} \right\| \leq const \ \lambda_{12}(\epsilon, \alpha)^t \,. \tag{8.44}$$

$\Diamond$

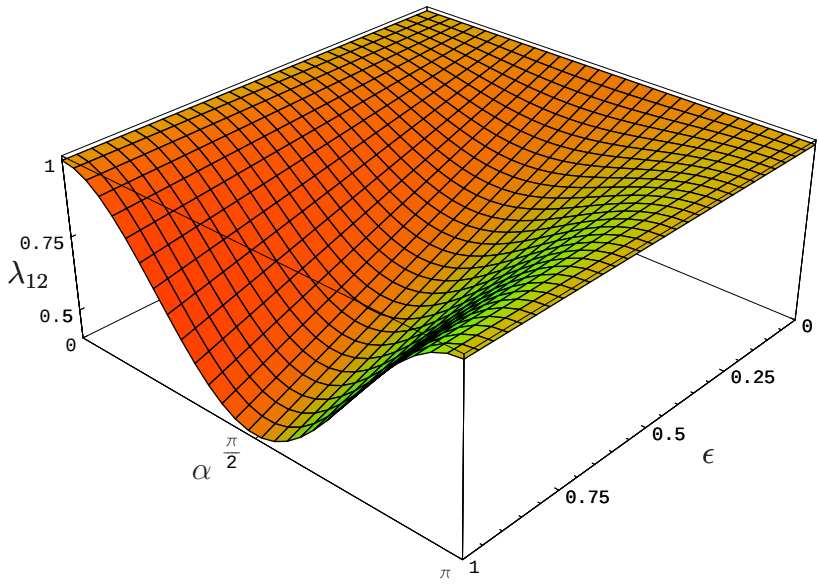

Figure 8.6: *Contraction rate λ_{12} in dependence of the noise parameters α and ϵ.*

Now the question is, what this contraction implies for the propagation behavior. It is easy to see that even the undisturbed walk does not show ballistic behavior when the initial state is totally mixed. This follows because the trace of the velocity operator in Eq. (2.30) vanishes. Therefore the loss of information in the internal degree of freedom can be thought of as first order process, which then leads to diffusive propagation behavior.

8.5 Conclusions and Outlook

In this Chapter we have studied the structure and the asymptotic behavior of decoherent quantum walks. We have characterized translationally invariant completely positive maps in momentum space. We found that the corresponding Kraus operators possibly contain a momentum shift, which breaks the translation symmetry of the Kraus operators.

In Section 8.3 we have studied elaborately the asymptotic behavior of the probability distribution of decoherent quantum walks. We have used perturbation theory for the computation of the moments of the position distribution for long times. First, we considered commuting Kraus operators, which can be handled by first order perturbation theory, and we have shown that in this case we can introduce a velocity operator analogously to an undisturbed walk. Thus, the asymptotic behavior is quantum-like unless the velocity operator vanishes. In the case of non-commuting Kraus operators we used second order perturbation theory to compute the variance of the resulting position distribution analytically. In particular, in the case of random unitary operations we found that the behavior is always diffusive, i.e. classical-like. Furthermore, we analyzed the decoherence effect of fluctuating coin parameters, e.g. we applied the achieved results to compute the variance of the position distribution in dependence of the fluctuation constant of the coin. These fluctuating parameters have been modeled by using an ancillary quantum system, which carries the information of the coin parameter. We have also demonstrated by example that if momentum shifts, i.e. position dependent phases, occur in the Kraus operators the behavior gets more classical-like.

Finally, we found that in the case for many decoherence processes, e.g. random unitaries, the first order process is given by mixing the coin degree of freedom. Since even the undisturbed Hadamard walk with a totally mixed state as initial state shows diffusive behavior, the loss of information of the coin degree of freedom then leads to classical-like behavior.

Here we have mainly described the general theory of decoherent quantum walks. The next step would be to find a realistic decoherence model of the experimental realization in Bonn and to compare the experimental data with simulated results. We have provided a first step towards a realistic model of this experiment by the model of fluctuating coin parameters.

Appendix A

Support algebras

Here we describe the concept of support algebras, which have been introduced in [SW04]. Support algebras are an important tool in Chapter 3 and Chapter 5.

We start with a subalgebra $\mathcal{A} \subset \mathcal{B}_1 \otimes \mathcal{B}_2$ of a tensor product and we want to find the smallest C^*-algebra $\mathcal{S} \subset \mathcal{B}_1$ such that $\mathcal{A} \subset \mathcal{S} \otimes \mathcal{B}_2$. This will be done in two steps. First we think of the linear structure. We can uniquely expand every $A \in \mathcal{A}$ into a linear combination $A = \sum_\mu a_\mu \otimes e_\mu$, where $\{e_\mu\}$ is a fixed basis of $\mathcal{B}_2$. Then we define the *support* $s(\mathcal{A}, \mathcal{B}_1) \subset \mathcal{B}_1$ as the span of all the a_μ, which are needed in this expansion. A more formal definition is seen from another way: we can apply a linear functional on the second tensor factor, e.g. the partial trace, which gives an element of the support on the first factor, i.e. we can define

$$s(\mathcal{A}, \mathcal{B}_1) = \{id_{\mathcal{B}_1} \otimes \phi(A) | A \in \mathcal{A},\ \phi \in \mathcal{B}_2^*\}, \tag{A.1}$$

where * denotes the dual space of some algebra, i.e. the space of linear functionals. Analogous definitions can be done for the other tensor factor or with more tensor factors. Of course all elements of the supports suffice to expand every $A \in \mathcal{A}$, so we have

$$\mathcal{A} \subset s(\mathcal{A}, \mathcal{B}_1) \otimes s(\mathcal{A}, \mathcal{B}_2) \subset \mathcal{B}_1 \otimes \mathcal{B}_2. \tag{A.2}$$

Now we want to build algebras out of these supports. The support is a linear subspace of a C^*-algebra, therefore we can define the *support algebra* $S(\mathcal{A}, \mathcal{B}_i) \subset \mathcal{B}_i$ of $\mathcal{A} \subset \bigotimes_i \mathcal{B}_i$ on one factor $\mathcal{B}_i$ as the algebra generated by the elements of $s(\mathcal{A}, \mathcal{B}_i)$ and of course we have

$$\mathcal{A} \subset S(\mathcal{A}, \mathcal{B}_1) \otimes S(\mathcal{A}, \mathcal{B}_2) \subset \mathcal{B}_1 \otimes \mathcal{B}_2. \tag{A.3}$$

In particular $S(\mathcal{A}, \mathcal{B}_1)$ is the smallest C^*-subalgebra $\mathcal{S} \subset \mathcal{B}_1$ such that $\mathcal{A} \subset \mathcal{S} \otimes \mathcal{B}_2$.

There are some almost obvious properties of support algebras. For instance, if we have a support algebra $S(\mathcal{A}, \mathcal{B}_1 \otimes \mathcal{B}_2) \subset \mathcal{B}_1 \otimes \mathcal{B}_2$ on two tensor factors, it is clear that this algebra is contained in the tensor product of the single algebra tensor factors, i.e.

$$S(\mathcal{A}, \mathcal{B}_1 \otimes \mathcal{B}_2) \subset S(\mathcal{A}, \mathcal{B}_1) \otimes S(\mathcal{A}, \mathcal{B}_2). \tag{A.4}$$

If we have two algebras $\mathcal{A}_1, \mathcal{A}_2 \subset \mathcal{B}_1 \otimes \mathcal{B}_2$ we have

$$S(\mathcal{A}_1 \vee \mathcal{A}_2, \mathcal{B}_1) = S(\mathcal{A}_1, \mathcal{B}_1) \vee S(\mathcal{A}_2, \mathcal{B}_1), \tag{A.5}$$

where $\mathcal{A}_1 \vee \mathcal{A}_2$ denotes the C^*-algebra generated by the algebras $\mathcal{A}_1$ and $\mathcal{A}_2$, because both sides of the equation are just the smallest C^*-algebra $\mathcal{S} \subset \mathcal{B}_1$ such that both $\mathcal{A}_1 \subset \mathcal{S} \otimes \mathcal{B}_2$ and $\mathcal{A}_2 \subset \mathcal{S} \otimes \mathcal{B}_2$.

For the constructive approach of the index theory of QCAs (Chapter 3) and for many results of Chapter 5 we need the following Lemma:

Lemma A.1 *Consider the subalgebras $\mathcal{A}_1 \subset \mathcal{B}_1 \otimes \mathcal{B}_2$ and $\mathcal{A}_2 \subset \mathcal{B}_2 \otimes \mathcal{B}_3$ such that $\mathcal{A}_1 \otimes \mathbb{1}_3$ and $\mathbb{1}_1 \otimes \mathcal{A}_2$ commute in $\mathcal{B}_1 \otimes \mathcal{B}_2 \otimes \mathcal{B}_3$. Then the support algebras $S(\mathcal{A}_1, \mathcal{B}_2)$ and $S(\mathcal{A}_2, \mathcal{B}_2)$ commute in $\mathcal{B}_2$.*

Proof: Pick bases $\{e_\mu\} \subset \mathcal{B}_1$ and $\{e'_\nu\} \subset \mathcal{B}_3$ and let $a \in \mathcal{A}_1$ and $a' \in \mathcal{A}_2$. We can expand uniquely into $a = \sum_\mu e_\mu \otimes a_\mu$ and $a' = \sum_\nu a'_\nu \otimes e_\nu$. Then by assumption we have

$$0 = [a \otimes \mathbb{1}_3, \mathbb{1}_1 \otimes a'] = \sum_{\mu,\nu} e_\mu \otimes [a_\mu, a'_\nu] \otimes e'_\nu$$

Since $\{e_\mu \otimes e'_\nu\}_{\mu,\nu}$ is a basis of $\mathcal{B}_1 \otimes \mathcal{B}_3$, this expansion is unique and forces a_μ and a'_ν to commute. This property also transfers to the algebras generated by these operators, i.e., to the support algebras noted in the Lemma. ■

The crucial point on this Lemma is, that $\mathcal{B}_2$ contains the whole overlap of the algebras $\mathcal{A}_1$ and $\mathcal{A}_2$. If we have for instance commuting subalgebras $\mathcal{A}_1 \subset \mathcal{B}_1 \otimes \mathcal{B}_2 \otimes \mathcal{B}_3$ and $\mathcal{A}_2 \subset \mathcal{B}_2 \otimes \mathcal{B}_3 \otimes \mathcal{B}_4$ then we do not know that the support algebras $S(\mathcal{A}_1, \mathcal{B}_2)$ and $S(\mathcal{A}_2, \mathcal{B}_2)$ commute and most times they will not do this.

Appendix B

Some Lemmata

For the proofs of Chapter 8 the following Lemma turns out to be very useful.

Lemma B.1 *Let W be a decoherent quantum walk, i.e., $W(A) = \sum_{j=1}^{m} K_j^* A K_j$. Then, $W(A) = A$ holds if and only if A commutes with all the Kraus operators K_j.*

Proof: " $\Leftarrow$ " This direction is trivial.
" $\Rightarrow$ " The condition $W(A) = A$ yields

$$\sum_{j=1}^{m} [K_j, A]^* [K_j, A] = W(A^*A) - A^*A\,.$$

Since the walk itself is trace-preserving, the trace of the right hand side of this equation is equal to zero. On the left hand side, we have a sum of positive operators, since X^*X is always positive. Thus, they all have to be zero, i.e., $[K_j, A] = 0$ for all j. ■

If all the Kraus operators commute, they can all be expanded in the same eigenbasis. A can then be, too. If they all do not commute among each other, such that there is no invariant subspace, then $A =$ must hold.

Furthermore, we need the following formula:

Lemma B.2 *For $a, b \in$,*

$$\lim_{t\to\infty} \left(1 + \frac{ia}{\sqrt{t}} + \frac{b}{t}\right)^t e^{-ia\sqrt{t}} = e^{\frac{a^2}{2}+b} \tag{B.1}$$

holds.

Proof: Expansion of the exponential function yields

$$\begin{aligned}\left(1+\frac{ia}{\sqrt{t}}+\frac{b}{t}\right)^t e^{-ia\sqrt{t}} &= \left(\left(1+\frac{ia}{\sqrt{t}}+\frac{b}{t}\right)e^{-ia/\sqrt{t}}\right)^t \\ &= \left(\left(1+\frac{ia}{\sqrt{t}}+\frac{b}{t}\right)\sum_{n=0}^{\infty}\frac{(-ia)^n}{\sqrt{t}^n n!}\right)^t \\ &= \left(1+\frac{a^2}{2t}+\frac{b}{t}+\frac{u_t}{t}\right)^t,\end{aligned}$$

where u_t contains all the remaining summands multiplied by the time t for which holds: $\lim_{t\to\infty}|u_t| = 0$. Thus, we obtain

$$\lim_{t\to\infty}\left(1+\frac{ia}{\sqrt{t}}+\frac{b}{t}\right)^t e^{-ia\sqrt{t}} = \lim_{t\to\infty}\left(1+\frac{\frac{a^2}{2}+b+u_t}{t}\right)^t = e^{\frac{a^2}{2}+b}.$$

■

Bibliography

[AAKV01] D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani. Quantum walks on graphs. In *Proc. of the 33rd ACM Symposium on Theory of computing*, pages 50–59, 2001.

[ABH+01] G. Alber, T. Beth, M. Horodecki, R. Horodecki, P. Horodecki, M. Rötteler, H. Weinfurter, R. F. Werner, and A. Zeilinger. *Quantum information – an introduction to basic theoretical concepts and experiments*. Springer, 2001.

[ABN+01] A. Ambainis, E. Bach, A. Nayak, A. Vishwanath, and J. Watrous. One-dimensional quantum walks. In *Proc. of the 33rd ACM Symposium on Theory of Computing*, pages 37–49, 2001.

[ADSS07] G. Abal, R. Donangelo, F. Severo, and R. Siri. Decoherent quantum walks driven by a generic coin operation. *Phys. A*, 387(1):335–345, 2007, arXiv:0708.1297.

[ADZ93] Y. Aharonov, L. Davidovich, and N. Zagury. Quantum random walks. *Phys. Rev. A*, 48(2):1687–1690, 1993.

[AFW07] P. Arrighi, R. Fargetton, and Z. Wang. Intrinsically universal one-dimensional quantum cellular automata in two flavours, 2007, arXiv:0704.3961v3.

[Amb03] A. Ambainis. Quantum walks and their algorithmic application. *Int. J. Quant. Inf.*, 1:507, 2003, quant-ph/0403120.

[Amb04] A. Ambainis. Quantum walk algorithm for element distinctness. In *Proc. 45th Annual IEEE Symposium on Foundations of Computer Science (FOCS'04)*, volume 0, pages 22–31, 2004, quant-ph/0311001.

[ANW08] P. Arrighi, V. Nesme, and R. F. Werner. Unitarity plus causality implies locality, 2008, arXiv:0711.3975v2.

[AP72] S. Amoroso and Y. N. Patt. Decision procedures for surjectivity and injectivity of parallel maps for tesselation structures. *J. Comp. Syst. Sci.*, 6:448–464, 1972.

[Arr06] P. Arrighi. An algebraic study of unitary one dimensional quantum cellular automata. In *Mathematical Foundations of Computer Science 2006*, volume 4162 of *Lecture Notes in Computer Science*, pages 122–133. 2006, quanth-ph/0512040.

[ASS90] J. Avron, R. Seiler, and B. Simon. Quantum Hall effect and the relative index for projections. *Phys. Rev. Lett.*, 65(17):2185, 1990.

[ASS94a] J. Avron, R. Seiler, and B. Simon. Charge deficiency, charge transport and comparison of dimensions. *Comm. Math. Phys.*, 159:399–422, 1994.

[ASS94b] J. Avron, R. Seiler, and B. Simon. The index of a pair of projections. *J. Funct. Anal.*, 120:220–237, 1994.

[BCA03a] T. A. Brun, H. A. Carteret, and A. Ambainis. Quantum random walks with decoherent coins. *Phys. Rev. A*, 67:032304, 2003, quant-ph/0210180.

[BCA03b] T. A. Brun, H. A. Carteret, and A. Ambainis. The quantum to classical transition for random walks. *Phys. Rev. Lett.*, 91:130602, 2003, quant-ph/0208195.

[BCA03c] T. A. Brun, H. A. Carteret, and A. Ambainis. Quantum walks driven by many coins. *Phys. Rev. A*, 67:052317, 2003, quant-ph/0210161.

[BCG82] E. R. Berlekamp, J. H. Conway, and R. K. Guy. *Winning Ways for Your Mathematical Plays*, volume 2. Academic Press, London, 1982.

[Ben00] S. C. Benjamin. Schemes for parallel quantum computation without local control of qubits. *Phys. Rev. A*, 61:020301, 2000, quant-ph/9909007.

[BF06] G. Birkl and J. Fortágh. Micro traps for quantum information processing and precision force sensing. *Laser & Photon. Rev.*, 1:12–23, 2006.

[BHV06] S. Bravyi, M. B. Hastings, and F. Verstraete. Lieb-Robinson bounds and the generation of correlations and topological quantum order. *Phys. Rev. Lett.*, 97:050401, 2006, quant-ph/0603121.

[BJ99] O. Bratteli and P. E. T. Jorgensen. Wavelet filters and infinite-dimensional unitary groups. In *Proc. of the Int. Conf. on Wavelet Analysis and Appl.* International Press, 1999, math/0001171v3.

[BR87] O. Bratteli and D. W. Robinson. *Operator algebras and quantum statistical mechanics*, volume I. Springer Verlag, 1987.

[BR97] O. Bratteli and D. W. Robinson. *Operator algebras and quantum statistical mechanics*, volume II. Springer Verlag, 1997.

[BRD+08] P. Barmettler, A. M. Rey, E. Demler, M. D. Lukin, I. Bloch, and V. Gritsev. Quantum many-body dynamics of coupled double-well superlattices. *Phys. Rev. A*, 78:012330, 2008, arXiv:0803.1643.

[Bro74] W. S. Brown. On euclid's algorithm and the computation of polynomial greatest common divisors. *J. Assoc. Comp. Mach.*, 18(4):478–504, 1974.

[BT96] B. M. Boghosian and W. Taylor. A quantum lattice-gas model for the many-particle Schroedinger equation, 1996, quant-ph/9604035v2.

[BT98] B. M. Boghosian and W. Taylor. Simulating quantum mechanics on a quantum computer. *Physica D*, 120:30, 1998, quant-ph/9701019.

[BW03] G. K. Brennen and J. E. Williams. Entanglement dynamics in one-dimensional quantum cellular automata. *Phys. Rev. A*, 68:042311, 2003, quant-ph/0306056.

[CIR03] H. A. Carteret, M. E. H. Ismail, and B. Richmond. Three routes to the exact asymptotics for the one-dimensional quantum walk. *J. Phys. A*, 36:8775, 2003, quant-ph/0303105.

[CK05] E. Czeizler and J. Kari. A tight linear bound on the neighborhood of inverse cellular automata. In *Automata, Languages and Programming*, volume 3580 of *Lecture Notes in Computer Science*, pages 410–420. 2005.

[CZ95] J. I. Cirac and P. Zoller. Quantum computations with cold trapped ions. *Phys. Rev. Lett.*, 74:4091, 1995.

[Dei78] P. A. Deift. Applications of a commutation formula. *Duke Mathematical Journal*, 45(2):267–310, 1978.

[DEO08] C. M. Dawson, J. Eisert, and T. J. Osborne. Unifying variational methods for simulating quantum many-body systems. *Phys. Rev. Lett.*, 100:130501, 2008, arXiv:0705.3456.

[Deu85] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. In *Proc. of the Royal Society of London*, volume A400, pages 97–117, 1985.

[DF04] F. Delgosha and F. Fekri. Results on the factorization of multidimensional matrices for paraunitary filterbanks over the complex field. *IEEE Trans. Signal Processing*, 52(5), 2004.

[DiV95] D. P. DiVincezo. Two-bit gates are universal for quantum computation. *Phys. Rev. A*, 51:1015, 1995, cond-mat/9407022.

[DiV00] D. P. DiVincezo. The physical implementation of quantum computation. *Fortschritte der Physik*, 48:771–783, 2000, quant-ph/0002077.

[DL95] J. O. Durand-Lose. Reversible cellular automaton able to simulate any other reversible one using partitioning automata. In *LATIN '95: Theoretical Informatics*, volume 911 of *Lecture Notes in Computer Science*, pages 230–244. 1995.

[DL01] J. Durand-Lose. Representing reversible cellular automata with reversible block cellular automata. In R. Cori, J. Mazoyer, M. Morvan, and R. Mosseri, editors, *Discrete Models: Combinatorics, Computation, and Geometry, DM-CCG 2001*, volume AA of *DMTCS Proceedings*, pages 145–154. Discrete Mathematics and Theoretical Computer Science, 2001.

[DRKB02] W. Dür, R. Raussendorf, V. Kendon, and H.-J. Briegel. Quantum random walks in optical lattices. *Phys. Rev. A*, 66:052319, 2002, quant-ph/0207137.

[DS96] C. Dürr and M. Santha. A decision procedure for unitary linear quantum cellular automata. In *IEEE Symposium on Foundations of Computer Science*, pages 38–45, 1996, quanth-ph/9604007.

[DS98] I. Daubechies and W. Sweldens. Factoring wavelet transforms into lifting steps. *J. Four. Anal. Appl.*, 4(3), 1998.

[DTS97] C. Dürr, H. Lê Thanh, and M. Santha. A decision procedure for well-formed linear quantum cellular automata. *Random Struct. Algorithms*, 11(4):381–394, 1997, cs.DS/9906024.

[EO06] J. Eisert and T. J. Osborne. General entanglement scaling laws from time evolution. *Phys. Rev. Lett.*, 97:150404, 2006, quant-ph/0603114.

[Fel57] W. Feller. *An introduction to probability theory and its applications*, volume I. John Wiley & Sons, Inc., 1957.

[Fey82] R. P. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467–488, 1982.

[FG98] E. Farhi and S. Gutmann. Quantum computation and decision trees. *Phys. Rev. A*, 58:915–928, 1998.

[FH04a] E. Feldman and M. Hillery. Quantum walks on graphs and quantum scattering theory. In *Proc. of the Conf. on Coding Theory and Quantum Computing*, 2004, quant-ph/0403066.

[FH04b] E. Feldman and M. Hillery. Scattering theory and discrete-time quantum walks. *Phys. Lett. A*, 324:277, 2004, quant-ph/0312062.

[FH07] E. Feldman and M. Hillery. Modifying quantum walks: A scattering theory approach. *J. Phys. A*, 40:11343–11359, 2007, arXiv:0705.4612.

[FNW92] M. Fannes, B. Nachtergaele, and R. F. Werner. Finitely correlated states on quantum spin chains. *Comm. Math. Phys.*, 144:443–490, 1992.

[FTC+07] S. Fölling, S. Trotzky, P. Cheinet, M. Feld, R. Saers, A. Widera, T. Müller, and I. Bloch. Direct observation of second-order atom tunnelling. *Nature*, 448:1029–1032, 2007.

[Gat05] A. Gattner. Asymptotisches Verhalten von Quanten-Zellularautomaten. Master's thesis, Institut für Mathematische Physik, TU Braunschweig, Germany, 2005.

[GE07] D. Gross and J. Eisert. Novel schemes for measurement-based quantum computation. *Phys. Rev. Lett.*, 98:220503, 2007, quant-ph/0609149.

[GESPG07] D. Gross, J. Eisert, N. Schuch, and D. Perez-Garcia. Measurement-based quantum computation beyond the one-way model. *Phys. Rev. A*, 76:052315, 2007, arXiv:0706.3401.

[GJS04a] A. D. Gottlieb, S. Janson, and P. F. Scudo. Convergence of coined quantum walks on d-dimensional euclidean space, 2004, quant-ph/0406072.

[GJS04b] G. Grimmett, S. Janson, and P. Scudo. Weak limits for quantum random walks. *Phys. Rev. E*, 69:026119, 2004, quant-ph/0309135.

[GME+02] M. Greiner, O. Mandel, T. Esslinger, T. W. Hänsch, and I. Bloch. Quantum phase transition from a superfluid to a Mott insulator in a gas of ultracold atoms. *Nature*, 415:39–44, 2002.

[Got97] D. Gottesman. *Stabilizer Codes and Quantum Error Correction*. PhD thesis, Caltech, 1997, quant-ph/9705052.

[Güt08] J. Gütschow. Cliffordkanäle als Zellularautomaten und Faltungskodierer. Master's thesis, TU Braunschweig, 2008.

[GZ88] G. Grössing and A. Zeilinger. A conservation law in quantum cellular automata. *Physica D*, 31:70, 1988.

[Has07] M. B. Hastings. Entropy and entanglement in quantum ground states. *Phys. Rev. B*, 76:035114, 2007, cond-mat/0701055.

[Hed69] G. A. Hedlund. Endomorphisms and automorphisms of the shift dynamical system. *Math. Syst. Theory*, 3:320–375, 1969.

[HK06] M. B. Hastings and T. Koma. Spectral gap and exponential decay of correlations. *Comm. Math. Phys.*, 265:781–804, 2006, math-ph/0507008.

[Hol02] A. S. Holevo. Remarks on the classical capacity of quantum channel, 2002, quant-ph/0212025.

[Hol04] A. S. Holevo. Additivity conjecture and covariant channels. In *Proc. of the Conf. on Foundations of Quantum Information*, 2004.

[Jac75] N. Jacobsen. *Lectures in abstract algebra. Volume I: Basic Concepts*. Number 30 in Graduate Texts in Mathematics. Springer Verlag, 1975.

[JBC+99] D. Jaksch, H.-J. Briegel, J. I. Cirac, C. W. Gardiner, and P. Zoller. Entanglement of atoms via cold controlled collisions. *Phys. Rev. Lett.*, 82:1975, 1999, quant-ph/9810087.

[Jon83] V. F. R. Jones. Index for subfactors. *Invent. math.*, 72:1–25, 1983.

[Kar90] J. Kari. Reversibility of 2D cellular automata is undecidable. *Physica D*, 45:379–385, 1990.

[Kar96] J. Kari. Representation of reversible cellular automata with block permutaions. *Math. Syst. Theory*, 29:47–61, 1996.

[Kar05a] J. Kari. Reversible cellular automata. In *Developments in Language Theory*, volume 3572 of *Lecture Notes in Computer Science*, pages 57–68. 2005.

[Kar05b] J. Kari. Theory of cellular automata: A survey. *Theor. Comp. Sci.*, 334:3–33, 2005.

[Kat66] T. Kato. *Perturbation theory for linear operators*. Springer, 1966.

[Kay08] A. Kay. The computational power of symmetric Hamiltonians. *Phys. Rev. A*, 78:012346, 2008, arXiv:0801.3228.

[KBH06] J. Kosik, V. Buzek, and M. Hillery. Quantum walks with random phase shifts. *Phys. Rev. A*, 74:022310, 2006, quant-ph/0607092.

[Kem03] J. Kempe. Quantum random walks: an introductory overwiew. *Contemporary Physics*, 44:307–327, 2003, quant-ph/0303081.

[Ken06] V. Kendon. Decoherence in quantum walks - a review. *Math. Struct. Comp. Sci.*, 17:1169, 2006, quant-ph/0606016.

[Key02] M. Keyl. Fundamentals of quantum information theory. *Phys. Rep.*, 369, 2002.

[KFWM] M. Karski, L. Förster, A. Widera, and D. Meschede. Private communication.

[Kit05] A. Kitaev. Anyons in an exactly solved model and beyond. *Annals of Physics*, 321:2–111, 2005, cond-mat/0506438.

[KMSW06] M. Keyl, T. Matsui, D. M. Schlingemann, and R. F. Werner. Entanglement, Haag-duality and type properties of infinite quantum spin chains. *Rev. Math. Phys.*, 18:935–970, 2006, math-ph/0604071.

[KNS04] N. Konno, T. Namiki, and T. Soshi. Symmetry of distribution for the one-dimensional Hadamard walk. *Interdisc. Inf. Sci.*, 10:11, 2004, quant-ph/0205065.

[Kon05] N. Konno. A new type of limit theorems for the one-dimensional quantum random walk. *J. Math. Soc. Japan*, 57:1179, 2005, quant-ph/0206103.

[Kra83] K. Kraus. *States, effects and operations*. Lecturs Notes in Physics. Springer, 1983.

[KT02] V. Kendon and B. Tregenna. Decoherence in a quantum walk on the line, 2002, quant-ph/0210047.

[KT03a] V. Kendon and B. Tregenna. Decoherence can be useful in quantum walks. *Phys. Rev. A*, 67:042315, 2003, quant-ph/0209005.

[KT03b] V. Kendon and B. Tregenna. Decoherence in discrete quantum walks. In *Decoherence and Entropy in Complex Systems, Lecture Notes in Physics*, volume 633, pages 253–267. Springer, 2003, quant-ph/0301182.

[KV90] G. Karlsson and M. Vetterli. Theory of two-dimensional multirate filter banks. *IEEE Trans. Acoustics, Speech and Signal Processing*, 38(6):925–937, 1990.

[KW07] O. Krüger and R. F. Werner. Gaussian quantum cellular automata. In N. Cerf, G. Leuchs, and E. S. Polzik, editors, *Quantum Information with continuous variables of atoms and light*. Imperial College Press, 2007.

[Llo93] S. Lloyd. A potentially realizable quantum computer. *Science*, 261:1569–1571, 1993.

[LP03] C. C. López and J. P. Paz. Phase-space approach to the study of decoherence in quantum walks. *Phys. Rev. A*, 68:052305, 2003, quant-ph/0308104.

[LR72] E. H. Lieb and D. W. Robinson. The finite group velocity of quantum spin systems. *Comm. Math. Phys.*, 28:251–257, 1972.

[MAD+06] Y. Miroshnychenko, W. Alt, I. Dotsenko, L. Förster, M. Khudaverdyan, D. Meschede, D. Schrader, and A. Rauschenbeutel. An atom-sorting machine. *Nature*, 442:151, 2006.

[Mar84] N. Margolus. Physics-like models of computation. *Physica D*, 10:81–95, 1984.

[Mey96a] D. A. Meyer. From quantum cellular automata to quantum lattice gases. *J. Stat. Phys.*, 85:551–574, 1996, quant-ph/9604003.

[Mey96b] D. A. Meyer. On the absence of homogeneous scalar unitary cellular automata, 1996, quant-ph/9604011.

[Mey97a] D. A. Meyer. Quantum lattice gases and their invariants. *Int. J. Mod. Phys. C*, 8:717–735, 1997, quant-ph/9703027.

[Mey97b] D. A. Meyer. Quantum mechanics of lattice gas automata: One-particle plane waves and potentials. *Phys. Rev. E*, 55(5):5261–5269, 1997, quant-ph/9611005.

[Mey98] D. A. Meyer. Quantum mechanics of lattice gas automata: Boundary conditions and other inhomogeneities. *J. Phys. A*, 31:2321–2340, 1998, quant-ph/9712052.

[MGW+03a] O. Mandel, M. Greiner, A. Widera, T. Rom, T. W. Hänsch, and I. Bloch. Coherent transport of neutral atoms in spin-dependent optical lattice potentials. *Phys. Rev. Lett.*, 91:010407, 2003.

[MGW+03b] O. Mandel, M. Greiner, A. Widera, T. Rom, T. W. Hänsch, and I. Bloch. Controlled collisions for multiparticle entanglement of optically trapped atoms. *Nature*, 425:937–940, 2003.

[MH89] K. Morita and M. Harao. Computation universality of one-dimensional reversible (injective) cellular automata. *Trans. IEICE*, E 72(6):758–762, 1989.

[MLK77] M. Morf, B. Lévy, and S. Kung. New results in 2-D systems theory, part I: 2-D polynomial matrices, factorization and coprimeness. *Proceedings IEEE*, 65(6), 1977.

[MS98] D. McDuff and D. Salamon. *Introduction to Symplectic Topology.* Oxford Mathematical Monographs, 1998.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[NOS06] B. Nachtergaele, Y. Ogata, and R. Sims. Propagation of correlations in quantum lattice systems. *J. Stat. Phys.*, 124:1–13, 2006, math-ph/0603064.

[NS92] K. Nagel and M. Schreckenberg. A cellular automaton model for freeway traffic. *J. de Physique I*, 2:2221–2229, 1992.

[NS06] B. Nachtergaele and R. Sims. Lieb-Robinson bounds and the exponential clustering theorem. *Comm. Math. Phys.*, 265:119–130, 2006, math-ph/0506030.

[NV00] A. Nayak and A. Vishwanath. Quantum walk on the line, 2000, quant-ph/0010117.

[NW08] D. Nagaj and P. Woczan. Hamiltonian quantum cellular automata in 1D. *Phys. Rev. A*, 78:032311, 2008, arXiv:0802.0886.

[ÖR95] S. Östlund and S. Rommer. Thermodynamic limit of density matrix renormalization. *Phys. Rev. Lett.*, 75:3537, 1995.

[Osb06] T. J. Osborne. The dynamics of 1D quantum spin systems can be approximated efficiently. *Phys. Rev. Lett.*, 97:157202, 2006, quant-ph/0508031.

[Pas02] K. Paschen. *Über Reversibilität, Nicht-Determiniertheit und Quantenrechnen in Zellularautomaten*. PhD thesis, Universität Karlsruhe, 2002.

[Pau02] V. Paulsen. *Completely bounded maps and operator algebras*. Cambridge University Press, 2002.

[PDC05] C. A. Perez-Delgado and D. Cheung. Models of quantum cellular automata, 2005, quant-ph/0508164.

[PDC07] C. A. Perez-Delgado and D. Cheung. Local unitary quantum cellular automata. *Phys. Rev. A*, 76:032320, 2007, arXiv:0709.0006.

[Ple07] M. B. Plenio. Remarks on duality transformations and generalized stabilizer states. *J. Mod. Opt.*, 54:349, 2007, quant-ph/0703007.

[PLP+08] H. B. Perets, Y. Lahini, F. Pozzi, M. Sorel, R. Morandotti, and Y. Silberberg. Realization of quantum walks with negligible decoherence in waveguide lattices. *Phys. Rev. Lett.*, 100:170506, 2008, arXiv:0707.0741.

[Pre99] J. Preskill. Quantum information and computation, 1999. Lecture Notes for Physics 229, California Institut of Technology, Pasadena,.

[Rau05a] R. Raussendorf. A quantum cellular automaton for universal quantum computation. *Phys. Rev. A*, 72:022301, 2005, quant-ph/0412048.

[Rau05b] R. Raussendorf. Quantum computation via translation-invariant operations on a chain of qubits. *Phys. Rev. A*, 72:052301, 2005, quant-ph/0505122.

[RB01] R. Raussendorf and H.-J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188, 2001.

[RB02] R. Raussendorf and H.-J. Briegel. Computational model underlying the one-way quantum computer. *Quant. Inf. Comp.*, 6:433–486, 2002, quant-ph/0108067.

[Ric72] D. Richardson. Tesselations with local transformations. *J. Comp. Syst. Sci.*, 6:373–388, 1972.

[Roe96] J. Roe. *Index theory, coarse geometry, and topology of manifolds*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1996.

[Roe03] J. Roe. *Lectures on Coarse geometry*. American Mathematical Society, 2003.

[Ros62] M. Rosenblatt. *Random Processes*. Oxford University Press, 1962.

[RSA+05] A. Romanelli, R. Siri, G. Abal, A. Auyuanet, and R. Donangelo. Decoherence in the quantum walk on the line. *Phys. A*, 347C:137, 2005, quant-ph/0403192.

[RW95] S. Richter and R. F. Werner. Ergodicity of quantum cellular automata. *J. Stat. Phys.*, 82:963–998, 1995, cond-mat/9504001.

[SBBH03] D. Shapira, O. Biham, A. J. Bracken, and M. Hackett. One dimensional quantum walk with unitary noise. *Phys. Rev. A*, 68:062315, 2003, quant-ph/0309063.

[Sch04] D. M. Schlingemann. Cluster states, graphs and algorithms. *Quant. Inf. Comp.*, 4(4):287–324, 2004.

[Scu79] H. Scutaru. Some remarks on covariant completely positive maps. *Rep. Math. Phys.*, 16:79–87, 1979.

[SDK+04] D. Schrader, I. Dotsenko, M. Khudaverdyan, Y. Miroshnychenko, A. Rauschenbeutel, and D. Meschede. Neutral atom quantum register. *Phys. Rev. Lett.*, 93:150501, 2004, quant-ph/0409037.

[SFW06] D. J. Shepherd, T. Franz, and R. F. Werner. A universally programmable quantum cellular automaton. *Phys. Rev. Lett.*, 97:020502, 2006, quant-ph/0512058.

[Sho94] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proc. 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[Sho97] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Sci. Statist. Comput.*, 26:1484–1509, 1997, quant-ph/9508027.

[Sim96] B. Simon. *Representations of finite and compact groups*, volume 10 of *Graduate Studies in Mathematics*. American Mathematical Society, 1996.

[SK08] E. Segawa and N. Konno. Limit theorems for quantum walks driven by many coins. *Int. J. Quant. Inf.*, 6:1231–1243, 2008, arXiv:0807.5074.

[SKHR+03] F. Schmidt-Kaler, H. Häffner, M. Riebe, S. Gulde, G. P. T. Lancaster, T. Deuschle, C. Becher, C. F. Roos, J. Eschner, and R. Blatt. Realization of the Cirac-Zoller controlled–NOT quantum gate. *Nature*, 422:408, 2003.

[SKW03] N. Shenvi, J. Kempe, and K. B. Whaley. A quantum random-walk search algorithm. *Phys. Rev. A*, 67(5):052307, 2003.

[SVW08] D. M. Schlingemann, H. Vogts, and R. F. Werner. On the structure of Clifford quantum cellular automata. *J. Math. Phys.*, 49:112104, 2008, arXiv:0804.4447.

[SW04] B. Schumacher and R. F. Werner. Reversible quantum cellular automata. 2004, quant-ph/0405174.

[SWVC08] N. Schuch, M. M. Wolf, K.-G. H. Vollbrecht, and J. I. Cirac. On entropy growth and the hardness of simulating time evolution. *New J. Phys.*, 10:033032, 2008, arXiv:0801.2078.

[Tak03] M. Takesaki. *Theory of Operator Algebras III*, volume 127 of *Encyclopedia of Mathematical Sciences*. Springer, 2003.

[TD00] B. M. Terhal and D. P. DiVincenco. Problem of equilibration and the computation of correlation functions on a quantum computer. *Phys. Rev. A*, 61:022301, 2000, quant-ph/9810063v3.

[TM90] T. Toffoli and N. Margolus. Invertible cellular automata: A review. *Physica D*, 45:229–253, 1990.

[Tof77] T. Toffoli. Computation and construction universality of reversible cellular automata. *J. Comp. Syst. Sci.*, 15:213–231, 1977.

[Uph08] S. Uphoff. Stationary states of Clifford quantum cellular automata. Master's thesis, TU Braunschweig, 2008.

[VC04] F. Verstraete and J. I. Cirac. Renormalization algorithms for quantum-many body systems in two and higher dimensions, 2004, cond-mat/0407066.

[VC06] K. G. H. Vollbrecht and J. I. Cirac. Reversible universal quantum computation within translation invariant systems. *Phys. Rev. A*, 73:012324, 2006, quant-ph/0502143.

[VC08] K. G. H. Vollbrecht and J. I. Cirac. Quantum simulators, continuous-time automata, and translationally invariant systems. *Phys. Rev. Lett.*, 100:010501, 2008, arXiv:0704.3432.

[VD89] P. P. Vaidyanathan and Z. Doğanata. The role of lossless systems in modern digital signal processing: A tutorial. *IEEE Trans. Education*, 32:181–197, 1989.

[vD96] W. van Dam. Quantum cellular automata. Master's thesis, Computer Science Nijmegen, 1996.

[vN66] J. von Neumann. *Theory of Self-Reproducing Automata*. University of Illinois Press, Champaign, IL, USA, 1966.

[Vog05] H. Vogts. Quanten-Zellularautomaten mit lokalen Erhaltungsgrößen. Master's thesis, TU Braunschweig, 2005.

[VSB+01] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414:883887, 2001.

[VW01] K. G. H. Vollbrecht and R. F. Werner. Entanglement measures under symmetry. *Phys. Rev. A*, 64:062307, 2001, quant-ph/0010095.

[VWPGC06] F. Verstraete, M. M. Wolf, D. Perez-Garcia, and J. I. Cirac. Criticality, the area law, and the computational power of projected entangled pair states. *Phys. Rev. Lett.*, 96:220601, 2006, quant-ph/0601075.

[Wat95] J. Watrous. On one-dimensional quantum cellular automata. In *IEEE Symposium on Foundations of Computer Science*, pages 528–537, 1995.

[Wei80] J. Weidmann. *Linear operators on Hilbert spaces*. Springer, 1980.

[WGF+05] A. Widera, F. Gerbier, S. Fölling, T. Gericke, O. Mandel, and I. Bloch. Coherent collisional spin dynamics in optical lattices. *Phys. Rev. Lett.*, 95:190405, 2005.

[Wie08] K. Wiesner. Quantum cellular automata, 2008, arXiv:0808.0679.

[Wol02] S. Wolfram. *A new kind of science*. Wolfram Media, Inc., 2002.

[XGS01] T. Q. Nguyen X. Gao and G. Strang. On factorization of m-channel paraunitary filterbanks. *IEEE Trans. Signal Processing*, 49(7):1433–1446, 2001.

[Zha08] K. Zhang. The limiting distribution of decoherent quantum random walks, 2008, arXiv:0804.4311.

Acknowledgements

Now that I have written down the scientific stuff, which I have done over the last years, there is some time left to acknowledge the contributions of various people, who supported me in doing this whole work.

In the first place I would like to thank Reinhard F. Werner for introducing me to the field of quantum information, letting me join his research group and mentoring this thesis. It was also a great pleasure to assist his thermodynamics course, which helped me to fill some gaps in my knowledge.

Many thanks go to Michael Keyl for reviewing this thesis and for many interesting lectures, which definitely enriched the studies here in Braunschweig.

I would also like to thank Dirk Schlingemann for many discussions about mathematical problems and conspiracy theories during his time in Braunschweig and for continuing our joint work on Clifford quantum cellular automata.

I also enjoyed very much the work on quantum walks together with Annette Gattner, especially on the index stuff and on the irreversible walks.

During the time I had the pleasure to support our diploma students Sonja Uphoff, Johannes Gütschow and Norbert Warncke. Thanks for many inspiring discussions, which provided many new ideas for this thesis.

In the frame of the joint DFG project "Quantum Control and Simulation with Distributed Neutral Atom Systems" I enjoyed very much the mutual research group meetings and the upcoming discussions, in particular with the groups of Dieter Meschede from Bonn and Ignacio Cirac from Munich. Also thanks to Leonid Förster, Michal Karski and Artur Widera from Bonn for providing us with experimental data, which are now being analyzed.

Many thanks go to the members of the quantum information group in Braunschweig. Our former members Dirk Schlingemann, Ole Krüger, Dennis Kretschmann and Michael Reimpell I thank for kindly welcoming me to the group and helping me through the day's life at the IMaPh. I thank Andreas Ruschhaupt, Vincent Nesme, David Gross, Jukka Kiukas, Andre Ahlbrecht, Volkher Scholz, Albert Werner, Sönke Schmidt, Friederike Trimborn, Johannes Gütschow and all

the people, who left the group during the years, for many interesting scientific discussions and many amusing conversations. In particular, I thank Vincent for discussions on trying to formulate the index stuff as abstract as possible and David for bringing new insights into the theory. Many thanks go also to Conny Schmidt, not only for running the office and helping in administrative stuff, but also for permanent motivation and support. Special thanks go to Andre, Albert, Johannes, Volkher, Vincent and Conny for filling the breaks with table tennis, darts and table soccer. A draft of this thesis has been read by Andre, Albert, Johannes and Conny, whose feedback and corrections I appreciate a lot.

Special thanks go to Annette for sharing her life with me and supporting me throughout the time.

Funding from the Deutsche Forschungsgemeinschaft (DFG) in the frame of the "Forschergruppe 635" is gratefully acknowledged.